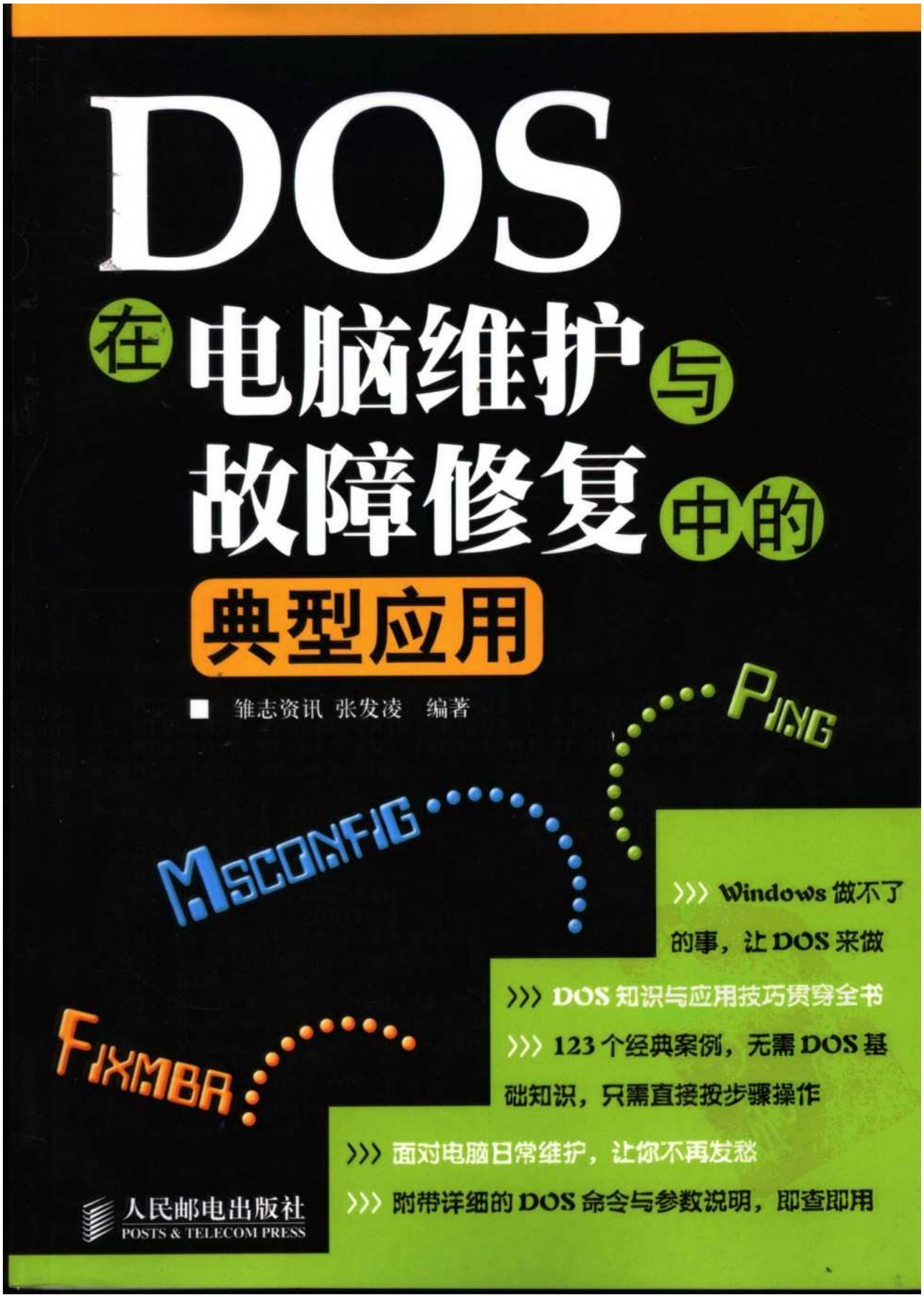
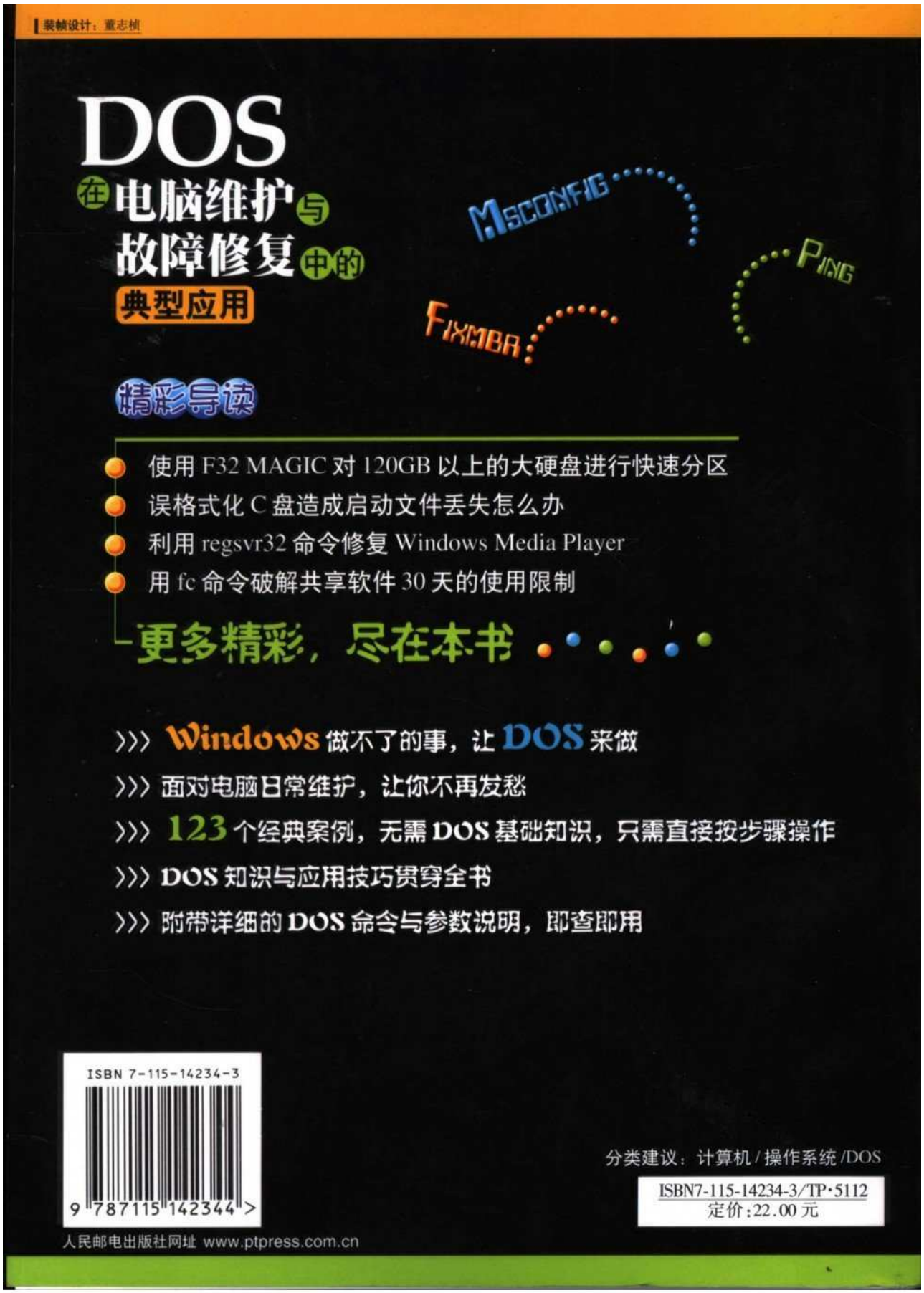
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



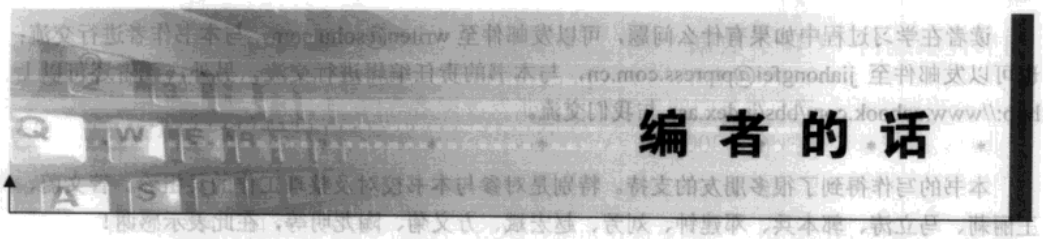
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



编者的话

前段时间有位朋友的电脑中了病毒，朋友忙活了半天也没能把病毒杀掉，后来一位“骨灰级”的电脑爱好者帮他除掉了病毒，朋友向我惊呼“杀毒竟然是在 DOS 下进行的”。我不禁哑然，难道 DOS 真的被人遗忘得这么彻底吗？

*　　*　　*　　*　　*　　*　　*　　*　　*

众所周知，真正有价值的东西是不会轻易退出历史舞台的。事实上，Windows 系统出现问题后，很多时候还是要借助 DOS 才能更好地解决，甚至有些问题不在 DOS 下是无法解决的。表面上已经屏蔽了 DOS（实模式）的 Windows 2000/XP/2003 系统，其内部反而集成了更多的 DOS 命令（保护模式），这也正说明了 DOS 的重要性。

在 DOS 下，我们其实可以进行很多非常实用的操作，比如修复硬盘坏道、恢复系统的分区表、找回误删除的文件、修复不能读取数据的软盘、解决网络故障等。我们也可以让 DOS 支持声卡、打印机、USB 接口等硬件设施。但是，对于很多读者，特别是没有经过“DOS 时代”的读者来说，DOS 还显得比较陌生。

很多人都说：高手之路，DOS 起步。DOS 知识对学习电脑操作的重要性由此可见一斑。为了让更多的读者了解 DOS 在今天的应用，我们组织编写了这本《DOS 在电脑维护与故障修复中的典型应用》。希望更多的读者能从本书中学习到解决电脑常见故障的方法。

*　　*　　*　　*　　*　　*　　*　　*　　*

本书主要介绍了 BIOS 刷新案例，硬盘分区、格式化经典案例，硬盘维护经典案例，Windows XP 系统维护经典案例，数据备份、恢复经典案例，故障恢复控制台救援经典案例，Windows 下的命令行，网络管理、维护经典案例，超级启动盘应用经典案例，以及 DOS 启动盘的制作、DOS 与 Windows 的共存、流行 DOS 工具软件的应用和 DOS 命令集。

在阅读过程中，读者会发现本书有以下几个特点。

- 开篇直接面对电脑应用中的常见问题，没有罗嗦的关于 DOS 的介绍。
- 以常见的问题（或任务）为驱动，详细介绍解决问题（或完成任务）的过程。
- 在介绍解决问题的办法时，穿插介绍 DOS 的相关知识和应用技巧。
- 附录中有比较完整的 DOS 命令列表，并有详细的参数讲解。

读者在阅读本书时，可以不用按章节顺序进行。本书的各个案例都是相对独立的，在知识上没有前后的关联，读者只要按照书中讲述的步骤进行操作即可。关于 DOS 的基础知识和操作技巧，本书并没有专门列出章节来单独介绍，而是融进了每一个案例的讲解中。本书所选的案例都有一定的代表性，读者在学习时举一反三，多实践，便可成为一名 DOS 应用高手。

本书的附录 D 分 4 个部分（DOS 的内外部命令、“批处理文件”命令、“系统恢复控制台”命令、“命令提示符”命令），较详细地介绍了 DOS 的命令集，并详细讲解了命令参数的作用。读者可以根据自己的需要查询 DOS 命令的用法。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

读者在学习过程中如果有什么问题，可以发邮件至 writen@sohu.com，与本书作者进行交流；也可以发邮件至 jiahongfei@ptpress.com.cn，与本书的责任编辑进行交流。另外，读者还可以上 http://www.ucbook.com/bbs/index.asp 与我们交流。

* * * * * * * * *

本书的写作得到了很多朋友的支持。特别是对参与本书校对及整理工作的吴祖珍、管文蔚、王丽莉、马立涛、郭本兵、邓建钟、刘芳、赵宏斌、方义菊、陶龙明等，在此表示感谢！

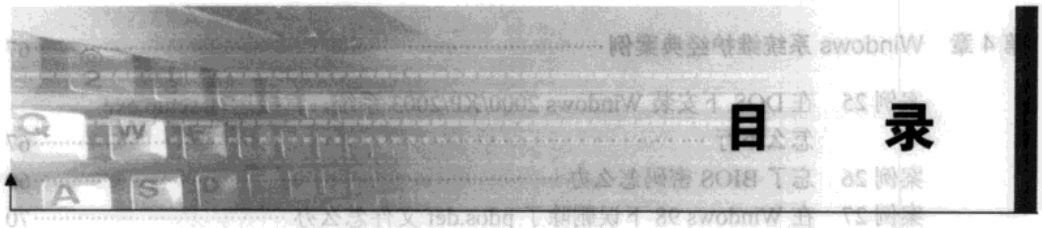
由于编者水平有限，书中难免有疏漏和不妥之处，读者若对本书有任何批评、指正或建议，欢迎与我们联系。

编者

2005 年冬

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



目　录

第 1 章　硬件 BIOS 刷新经典案例……1

案例 01　如何刷新 Award 的主板 BIOS 获得对新硬件的支持……1
案例 02　如何刷新 AMI 的主板 BIOS 以提高主板性能……3
案例 03　如何刷新 nVIDIA 显卡的 BIOS 解决兼容性问题……4
案例 04　如何刷新 ATI 显卡的 BIOS 提高性能……5
案例 05　如何刷新刻录机固件改善刻录性能……6
案例 06　如何刷新 DVD 固件解决区码限制问题……8

第 2 章　硬盘分区、格式化经典案例……11

案例 07　使用 fdisk 对硬盘进行分区与格式化……11
案例 08　使用 GDISK 对硬盘进行智能应答式分区与格式化……18
案例 09　使用 DM 对硬盘进行快速分区与格式化……24
案例 10　使用 PartitionMagic 对硬盘进行分区与格式化……29
案例 11　使用 Disk Genius 对硬盘进行分区与格式化……31
案例 12　使用 F32 MAGIC 对 120GB 以上大硬盘进行快速分区……37
案例 13　使用 Windows 2000/XP/2003 安装盘对硬盘进行分区……40

第 3 章　硬盘维护经典案例……43

案例 14　硬盘有坏道，系统不能引导、数据读取出错、系统频繁死机怎么办……43
案例 15　硬盘零磁道损坏，无法引导怎么办……46
案例 16　硬盘主引导扇区损坏，系统无法引导怎么办……49
案例 17　主引导扇区、分区表感染病毒，硬盘无法引导怎么办……51
案例 18　分区表被破坏，如何重建……55
案例 19　为什么不能对硬盘进行重新分区操作……57
案例 20　硬盘出现碎片，文件读取缓慢怎么办……59
案例 21　如何使用 NDD 扫描和修复磁盘错误……60
案例 22　如何使用 scandisk 修复磁盘中损坏的文件……62
案例 23　如何使用 chkdsk 检查和修复磁盘错误……64
案例 24　如何使用 Smartdrv 设置磁盘缓存加速……65

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 4 章　Windows 系统维护经典案例 ……67

案例 25　在 DOS 下安装 Windows 2000/XP/2003 系统，直接运行 setup.exe 怎么不行 ……67
案例 26　忘了 BIOS 密码怎么办 ……69
案例 27　在 Windows 98 下误删除了 pdos.def 文件怎么办 ……70
案例 28　系统文件被病毒感染后，在 Windows XP 下无法删除怎么办 ……71
案例 29　在 DOS 中，不能识别 NTFS 文件系统分区怎么办 ……71
案例 30　如何利用 PM（分区魔术师）将 NTFS 文件系统转换为 FAT32 文件系统 ……74
案例 31　如何利用 Disk Genius 将 FAT32 文件系统转换为 NTFS 文件系统 ……76
案例 32　在 DOS 下，如何对 NTFS 格式的分区的进行格式化 ……77
案例 33　如何完全卸载多操作系统中的 Windows XP ……78

第 5 章　DOS 下的经典应用案例 ……82

案例 34　使用 dir 命令查看目录中的文件时，屏幕滚动太快看不清楚内容怎么办 ……82
案例 35　在 DOS 下如何利用相对路径、绝对路径来创建或删除目录 ……85
案例 36　在 DOS 下如何删除垃圾文件和垃圾目录 ……87
案例 37　在 DOS 下如何来更改文件名 ……89
案例 38　在 DOS 下如何改变文件的属性 ……90
案例 39　在 DOS 下如何对磁盘分区进行高级格式化 ……91
案例 40　在 DOS 下忘记了某命令的基本格式和参数怎么办 ……92
案例 41　在 DOS 下如何利用重定向符来保存、输入、发送、打印件（<、>） ……94
案例 42　如何在 DOS 下执行更多的内外部命令 ……95
案例 43　在 DOS 下恢复误格式化分区中的文件 ……96

第 6 章　备份、恢复经典案例 ……99

案例 44　在 DOS 下备份、恢复主引导记录（MBR） ……99
案例 45　在 DOS 下备份、恢复分区表记录 ……102
案例 46　在 DOS 下手动备份、恢复注册表 ……104
案例 47　在 DOS 下利用注册表编辑器备份、恢复注册表 ……107
案例 48　在 DOS 下利用注册表检查器备份、恢复注册表 ……108
案例 49　在 DOS 下利用 Ghost 备份、恢复系统 ……109
案例 50　在 DOS 下利用 Ghost 备份、恢复分区映像 ……113
案例 51　在 DOS 下利用 Ghost 建立、恢复磁盘映像 ……115

第 7 章　Windows 2000/XP/2003 故障恢复控制台经典救援经典案例 ……119

案例 52　用安装光盘引导进入恢复控制台 ……119

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



案例 53　安装恢复控制台为启动菜单项……120
案例 54　系统启动时提示 ntfs.sys 文件丢失怎么办……120
案例 55　系统启动时提示 NTLDR 文件丢失怎么办……121
案例 56　误删了 SAM 文件怎么办……122
案例 57　多系统下 Windows XP 无法启动如何修复……123
案例 58　误格式化 C 盘造成启动文件丢失怎么办……124
案例 59　如何恢复损坏的 DLL 文件……125
案例 60　在恢复控制台下修复分区表……125
案例 61　如何格式化 NTFS 格式的系统盘……126
案例 62　如何从手动备份的注册表文件恢复注册表……126
案例 63　如何从系统自动备份的注册表文件修复注册表……127
案例 64　如何从故障恢复控制台清除木马病毒……128
案例 65　如何从故障恢复控制台替换修改了端口（135）的系统文件……128
案例 66　如何解除故障恢复控制台操作限制……129
案例 67　如何删除故障恢复控制台文件及启动菜单……130

第 8 章　Windows 窗口下的命令行……131

案例 68　如何快速启动系统自带的应用程序……131
案例 69　如何快速进入“准 DOS”窗口……132
案例 70　如何手工定制“定时关机”指令……132
案例 71　利用 regsvr32 命令修复 IE 浏览器……133
案例 72　利用 regsvr32 命令解决 Windows 无法在线升级的问题……134
案例 73　利用 regsvr32 命令防范网络脚本病毒……134
案例 74　利用 regsvr32 命令卸载 Windows XP 中不用的功能……134
案例 75　利用 regsvr32 命令给 WMP 注册 RM 插件……134
案例 76　利用 regsvr32 命令修复 Windows Media Player……135
案例 77　利用 regsvr32 命令修复“添加/删除程序”无法启动的问题……135
案例 78　利用 certmgr 命令解决 EFS 加密文件夹无法打开问题……135
案例 79　利用 winword 命令快速恢复 Word 设置……137
案例 80　利用 TASKKILL 命令快速结束程序进程……138
案例 81　利用 ntsd 命令关掉不明进程……138
案例 82　解决组策略被禁用的问题……139
案例 83　彻底清除 3721 实名程序……139
案例 84　用 fc 命令破解 30 天共享软件使用限制……140
案例 85　用 fc 命令辅助查杀 DLL 木马……140
案例 86　利用 netstat 命令查看本机开放端口……141
案例 87　用 netstat 命令查找打开可疑端口的恶意程序……141
案例 88　在 Windows XP 中用 netstat 命令直接查看端口与程序……142
案例 89　用 Fport 命令查看开放端口对应的程序……142



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

案例 90　用 Subst 命令无软盘安装软件……143
案例 91　停用“命令提示符”功能……143

第 9 章　网络管理、维护经典案例……145

案例 92　用 ping 命令诊断局域网故障……145
案例 93　借用 ping 命令定时运行程序……146
案例 94　用 tracert 命令了解本机与目标主机之间的数据传输路径……146
案例 95　用 arp 命令查看哪些计算机连接了本机……147
案例 96　用 nbtstat 命令探测对方计算机名……148
案例 97　用 nslookup 命令解决上网故障……149
案例 98　用 ipconfig 命令查看网络连接……150
案例 99　善用强大的 net 命令……151
案例 100　了解 at 命令是如何启动木马程序的……155
案例 101　用 at 命令设置计划任务……156
案例 102　用 telnet 命令远程连接计算机……157
案例 103　用 FTP 命令传输文件……158
案例 104　禁止 Windows 自带 TFTP 客户端的使用……158

第 10 章　超级启动盘应用经典案例……160

案例 105　引导计算机从 DOS 进入 Windows……160
案例 106　让 DOS 支持 USB 设备……161
案例 107　让 DOS 也能支持中文名显示……161
案例 108　让 DOS 支持长文件名……162
案例 109　让启动盘也能访问“网上邻居”……163

附录 A　DOS 启动盘的制作……166

案例 110　在 Windows 98 下制作启动盘……166
案例 111　在 DOS 下制作启动盘……167
案例 112　制作 Windows 2000 启动盘……167
案例 113　制作 Windows XP 启动盘……169
案例 114　制作 Windows XP 密码破解启动盘……169
案例 115　制作 USB 启动盘……170
案例 116　制作硬盘版 DOS 启动……171

附录 B　DOS 与 Windows 共存……174

案例 117　使用第三方工具来实现纯 DOS 与 Windows 系统共存……174
案例 118　安装 MS-DOS 7.10 来实现纯 DOS 与 Windows 系统共存……175
案例 119　手动设置实现纯 DOS 与 Windows 系统共存……181

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

附录 C　最新流行 DOS 工具软件应用指南……183

案例 120　矮人 XP2K 纯 DOS 模式 2.0……183
案例 121　梦幻中文 DOS 启动盘……185
案例 122　中文多功能 DOS 启动盘（识别闪存）3.0……186
案例 123　中文多功能 DOS 启动 U 盘……188

附录 D　命令集……191

一、DOS 内、外部命令……191
二、“批处理文件”命令……199
三、“系统恢复控制台”命令……200
四、“命令提示符”命令……205

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



第1章 硬件BIOS刷新经典案例

在DOS下刷新BIOS曾经是DOS下最经典的应用。现在，随着硬件厂家推出各类可以在Windows下刷新BIOS的工具，在DOS下进行BIOS刷新使用得相对少了。但是，对于一些较老的硬件产品，有时只能在DOS下才能刷新，所以掌握在DOS下刷新BIOS的操作方法是十分有必要的。

案例01 如何刷新Award的主板BIOS获得对新硬件的支持

升级主板BIOS首先要确定当前BIOS的型号和版本，其他硬件设备的BIOS或固件的升级也遵循相同的原则。错误的版本会导致刷新失败，甚至造成不可挽回的损失。

查看主板BIOS的详细信息可使用AIDA32这款软件，此软件的操作界面如图1-1所示。在界面左侧的“主板”类下，用户可以清晰地找到当前BIOS的厂家和版本信息，甚至可以直接单击下面厂商的网址下载BIOS升级程序。

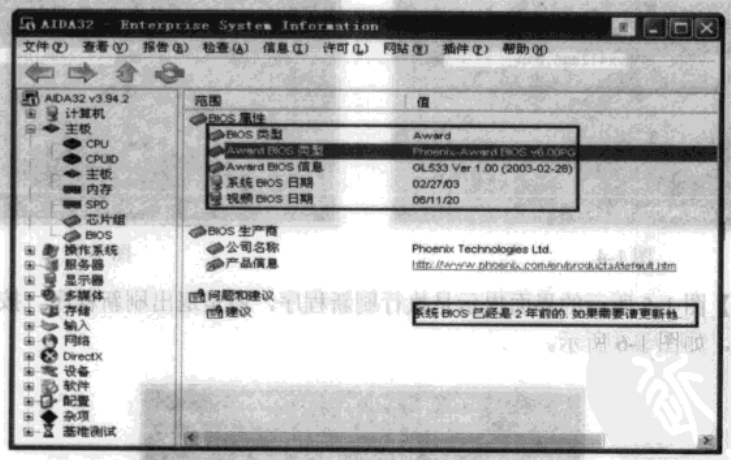


图1-1

确认了BIOS版本信息，就可以着手到厂家或其他专业网站下载正确的新版BIOS来刷新了。不过在刷新BIOS之前，一定要仔细阅读新版BIOS的信息。接下来根据下面的操作步骤完成刷新操作。

【第一步】制作一张软盘启动盘，将更新文件和更新程序一起拷贝到启动盘上（启动盘的制作，读者可以参考附录A中的内容）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

注意

（1）本例中复制的更新文件和更新程序，分别是 VX4L2AA6.BIN（BIOS 更新文件）和 AWD824G.EXE（BIOS 更新程序）。不同主板的 BIOS 更新文件名称不一定相同，具体的根据下载文件所得，而刷新程序大致是一样的。

（2）关于软盘启动盘的制作操作，读者可以参考附录 A 中的内容。

【第二步】用启动盘启动系统到 DOS 下，如图 1-2 所示。

【第三步】在提示符后输入 BIOS 升级指令，如“awd824g vx412226.bin /f”，按回车键，如图 1-3 所示。

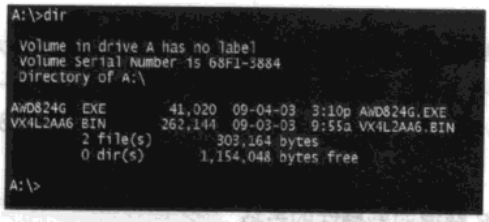


图 1-2

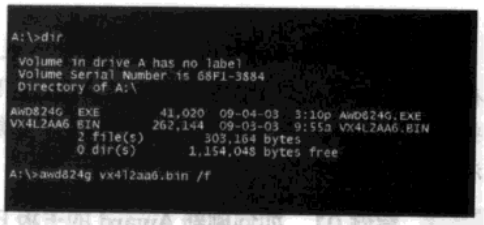


图 1-3

【第四步】接着进入到图 1-4 所示的界面中。提示用户是按“Y”键将旧的 BIOS 文件备份到磁盘上，还是按“N”键不进行旧 BIOS 文件的备份。

【第五步】若需要对旧 BIOS 文件进行备份，则按“Y”键，进入如图 1-5 所示的界面。

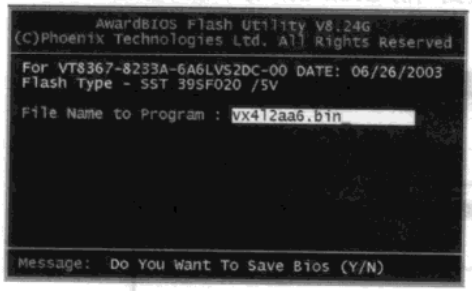


图 1-4

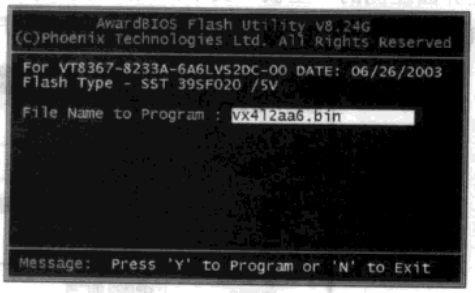


图 1-5

【第六步】图 1-5 所示的界面提示是执行刷新程序，还是退出刷新程序。按“Y”键，开始刷新 BIOS，如图 1-6 所示。



图 1-6

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

【第七步】刷新完成后，取出磁盘，按“F1”键继续，系统将重新启动。启动时按“DEL”键进入 BIOS，载入默认设置，并改变启动方式为从硬盘启动。

【第八步】退出 BIOS 设置，重新启动计算机即可。

案例 02 如何刷新 AMI 的主板 BIOS 以提高主板性能

刷新 AMI 主板 BIOS，同样先确认自己使用的主板上的 BIOS 版本，接下来到厂家或其他专业网站下载正确的新版 BIOS，然后根据下面的步骤完成刷新操作。

【第一步】制作一张启动盘，将更新文件和更新程序一起拷贝到启动盘上。

【第二步】用启动盘启动系统到 DOS 下。

【第三步】在提示符后输入升级指令，如“aminf330 020429.ROM”，按回车键，如图 1-7 所示。

【第四步】接着屏幕上显示如图 1-8 所示的信息，再次检查新的 BIOS 文件是否正确。

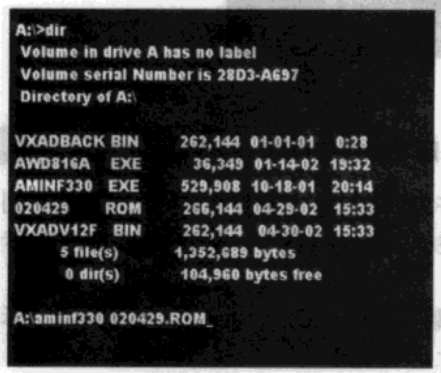


图 1-7

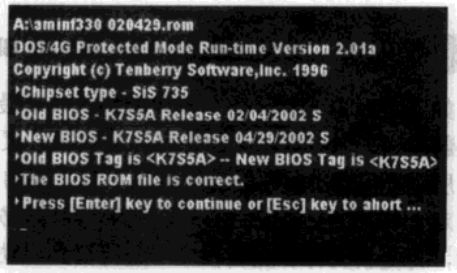


图 1-8

【第五步】若要刷新 BIOS，直接按回车键；若要退出刷新程序，按 Esc 键。按回车键后，程序开始刷新 BIOS，并等待刷新完成，如图 1-9 所示。

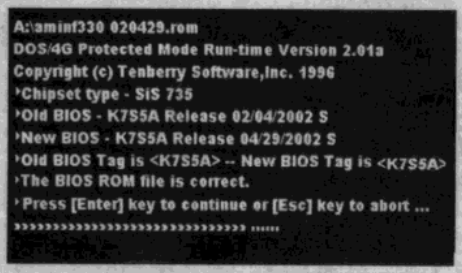


图 1-9

【第六步】刷新完毕重新启动系统，系统启动时按 Del 键进入 BIOS 设置，载入默认值，并将系统启动方式设为从硬盘启动。

【第七步】取出磁盘，退出 BIOS，再次重新启动系统即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

注意

主板类型的不同，刷新 BIOS 时也存在差异；有些主板厂家对 BIOS 刷新的支持比较完善，例如某 p4c81006 主板 BIOS 刷新程序，只需要在命令提示符后直接输入可执行文件，即可完成主板 BIOS 的刷新，如图 1-10 所示。这种情况是主板厂家已经把刷新文件和刷新程序集成到一起了，其刷新程序相当于一个批处理文件；而另一种情况就是上面的例子，用户需要手动输入刷新命令和刷新文件。

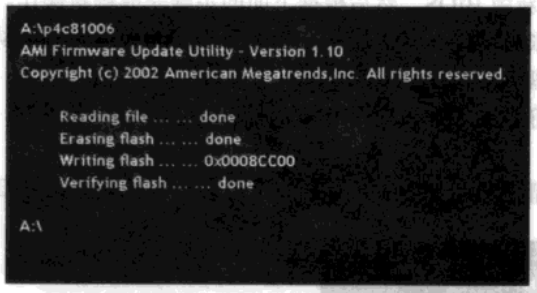


图 1-10

案例 03　如何刷新 nVIDIA 显卡的 BIOS 解决兼容性问题

如同主板 BIOS 一样，一种类型的显卡最初开发的 BIOS 总是存在缺陷，将其刷新到厂家最新改进的 BIOS，这样既可弥补缺陷，又可获得性能上的提升，甚至升级到新的显卡核心。所以，显卡 BIOS 的升级也是十分必要的。

对于 nVIDIA 显卡 BIOS 的升级，同样是先下载正确的 BIOS 更新文件，然后制作一张启动盘，将更新文件和更新程序一起拷贝到启动盘上。

nVIDIA 显卡 BIOS 的刷新使用 nvflash 程序，直接运行即可显示该程序的使用方法，如图 1-11 所示。

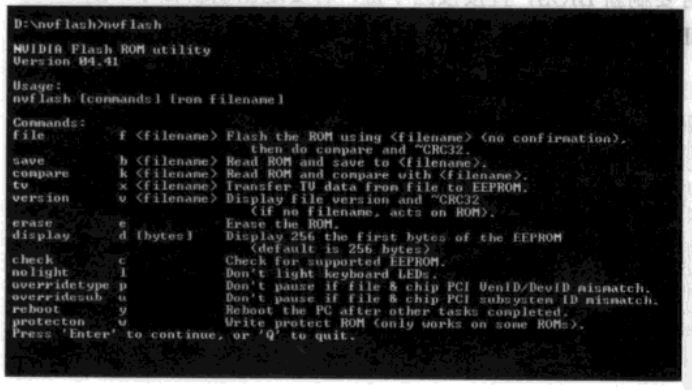


图 1-11

具体的 nVIDIA 显卡 BIOS 刷新步骤如下。

【第一步】备份显卡的 BIOS 文件。在提示符后输入“nvflash –b oldbios.bin”，按回车键。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

【第二步】运行刷新指令，在提示符后输入“nvflash -f newbios.bin”，按回车键。也可通过参数将新的 BIOS 文件刷入显卡，只需在提示符后输入“nvflash -p -u -f bios.bin”，按回车键即可。

【第三步】刷新完成后，重新启动计算机即可。

注意 不同版本的显卡 BIOS 刷新程序，在使用时所输入的指令可能不一样，如 nv4flash 刷新程序，应在提示符后输入“nv4flash 32090115.rom”，按回车键，如图 1-12 所示。

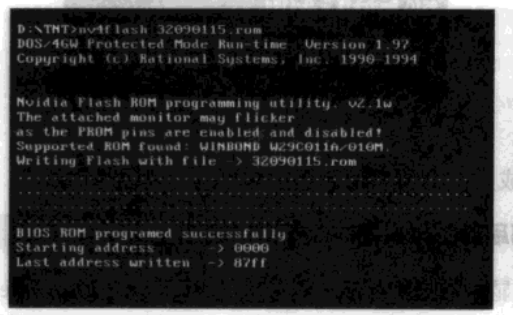


图 1-12

案例 04 如何刷新 ATI 显卡的 BIOS 提高性能

要刷新 ATI 显卡的 BIOS，先下载显卡 BIOS 的更新文件，然后制作一张启动盘，将更新文件和更新程序一起拷贝到启动盘上。

ATI 显卡 BIOS 的显卡更新程序推荐使用 ATIFlash，直接输入“atiflash”，按回车键即可看到该程序的使用方法，如图 1-13 所示。

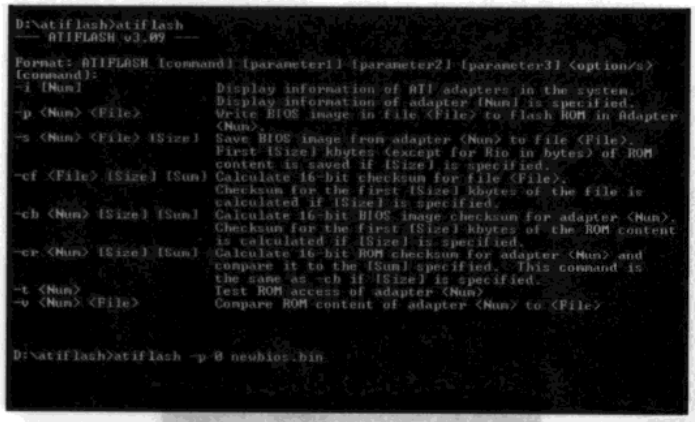


图 1-13

刷新 ATI 显卡 BIOS 的步骤如下。

【第一步】备份旧 BIOS 文件。在提示符后输入“atiflash –s 0 oldbios.bin”，按回车键。

【第二步】运行刷新命令。在提示符后输入“atiflash –p -0 newbios.bin”，按回车键。也可

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

以强制将一个新 BIOS 文件刷入显卡，只需要在提示符后输入“atiflash -f -p 0 bios.bin ”，按回车键即可，如图 1-14 所示。

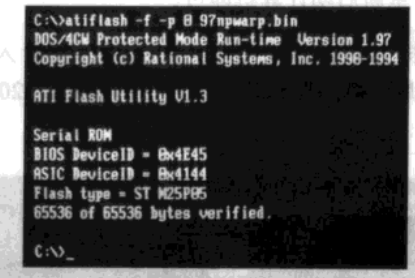


图 1-14

【第三步】刷新完成后，重新启动计算机即可。

案例 05 如何刷新刻录机固件改善刻录性能

如同主板 BIOS 和显卡 BIOS 一样，刻录机的 BIOS——Firmware（固件）也存在刷新的必要，当刻录机的刻录能力下降或对盘片挑剔时，通过刷新 BIOS 或许就能解决问题。

准备一张 DOS 启动盘，将下载好的正确的固件升级文件解压至软盘中。从软盘启动进入 DOS 后，建议先备份当前的刻录机固件文件。不同品牌的刻录机的刷新程序也不一样，在刷新 BIOS 时的方法也大不相同，下面介绍几种较为常见的升级刻录机 BIOS 的方法。

1. 利用批处理文件来刷新

有些下载的升级程序含有一个批处理文件，这种情况只需运行批处理文件，即可完成刷新，无需使用命令格式，如图 1-15 所示。

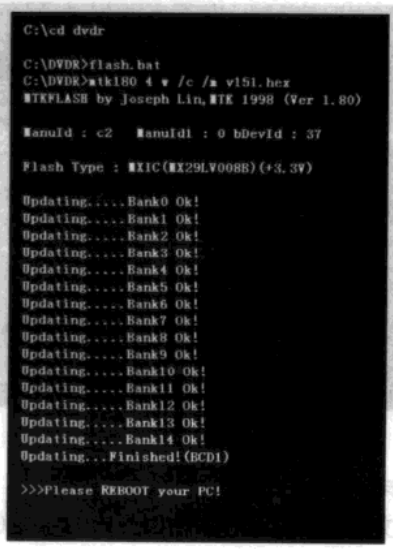


图 1-15

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

键入固件升级的批处理文件“flash.bat<回车>”，升级工具自动运行并刷新刻录机固件；等待数十秒后屏幕提示“Please REBOOT your PC!”并重新回到“C:\”提示符下。

重新启动电脑，即可完成固件升级。

2. 利用固件指令来刷新

【第一步】在提示符后输入刷新指令“dvflash dv1.bin”，按回车键，如图 1-16 所示。

【第二步】提示用户选择刻录机，如图 1-17 所示。

【第三步】选择好后，刷新将自动完成，如图 1-18 所示。

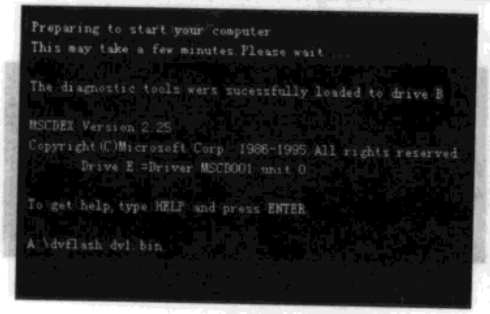


图 1-16

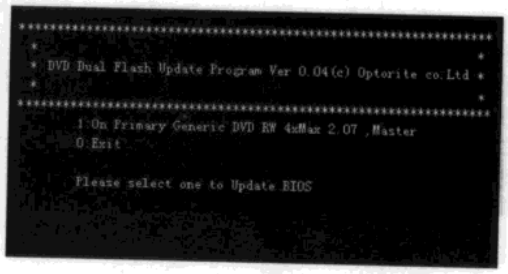


图 1-17

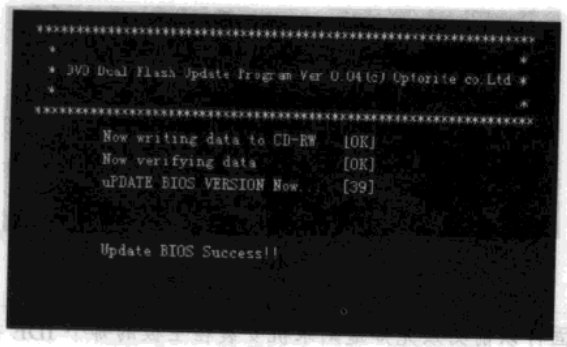


图 1-18

【第四步】重新启动系统。

3. 利用刷新程序来刷新

【第一步】在提示符后输入刷新指令，如“DVRFlash -v E: R7100007.105 R7100107.105”，按回车键。其中“E:”为光驱代号，R7100007.105 为 Kernel（核心）文件，R7100107.105 为升级的 Firmware 文件，如图 1-19 所示。

【第二步】在弹出提示信息后输入“y”，按回车键，显示 Firmware 文件及光驱信息，如图 1-20 所示。

【第三步】再输入“y”，按回车键，转换到 Kernel mode（核心模式），如图 1-21 所示。此时开始写入升级的 Firmware 文件，此步骤大约需要 30 秒，如图 1-22 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

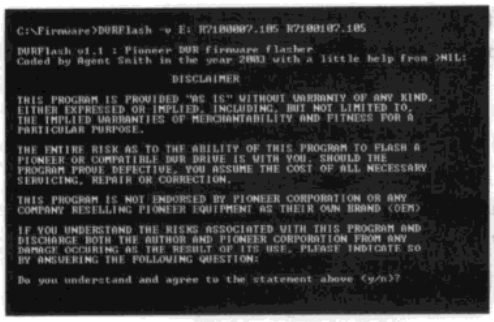


图 1-19

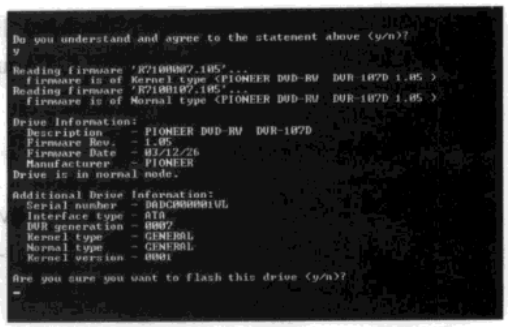


图 1-20

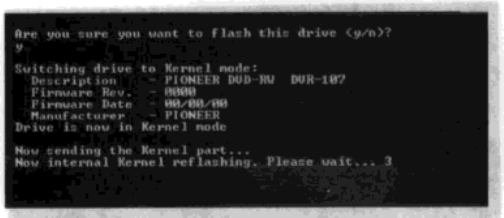


图 1-21

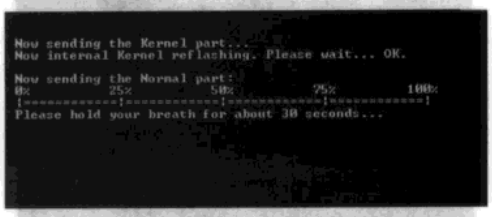


图 1-22

【第四步】系统显示更新成功及更新后的光驱信息，如图 1-23 所示。

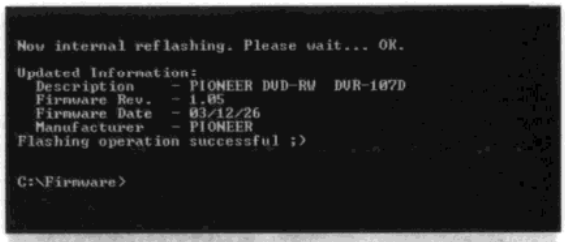


图 1-23

注意 在刷新固件以前必须先知道刻录机安装在主板的哪个 IDE 接口，因为 DOS 版的固件刷新程序不会自动寻找合适的 IDE 通道。

如果在 DOS 环境下升级时出现“Drive Not Responding Correctly”的字样，可多试几次。

虽然 DOS 版的升级程序比较麻烦，但是在 Windows 系统下升级不成功或出现问题，DOS 版的 Flash 程序也许能将用户的 DVD 刻录机挽救回来。

案例 06 如何刷新 DVD 固件解决区码限制问题

为了保护知识产权，很多 DVD 碟片有区码限制，相应的 DVD 光驱也锁定了区码。而光驱里的 Firmware 就具备识别区码的功能，当 DVD 碟片区码和光驱中的区码一致时，光驱就能读数据；否则，就报出错误信息。

为了破解 DVD 光驱的区码限制，一般有两种方法：一是硬件方法，通过刷新固件达到破解目的；另一种是软件方法，利用软件骗过 Firmware 的区码检测。这里介绍如何通过刷新

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Firmware 来解决问题。

如果用户的光驱使用的是 MTK 芯片，那么值得庆幸，可以说这是一种几乎没有刷新失败风险的控制芯片。采用了这种芯片的光驱，在固件刷新失败后可以很容易地修复（重新刷一次就可以了）。可以使用的刷新软件有 MTKFlash 和 MTKWinFlash，前者是 DOS 下的刷新工具，如图 1-24 所示；而后者是在 Windows 下的刷新工具。



图 1-24

MTKFlash 虽然是 DOS 下使用的刷新工具，但是功能很强。用户可以在刷新之前先备份光驱 Firmware，在刷新到新的 Firmware 后，若发现有什么问题，可以利用备份恢复过来。如果用户在 Firmware 还有 5 次区码修改机会的时候将其备份，当 DVD-ROM 被锁区后，只要把备份的 Firmware 刷回去，就又有了 5 次修改的机会。

1. 备份 Firmware

用 MTKFlash 备份 Firmware 的命令格式是：mtkflash port r /b /m backup.bin，其中 port 有 4 种选项参数。

- 1：First IDE master。
- 2：First IDE slave。
- 3：Second IDE master。
- 4：Second IDE slave。

如果光驱接在第二个 IDE 口上，而且是主盘的话，值就是 3。那么备份的命令格式是：mtkflash 3 r /b /m sso.bin（这里的 sso.bin 是备份文件的名称）。

参数说明如下。

- port：表示是 IDE 端口号。
- r：代表读（备份）。
- /b：代表保存为二进制文件（.bin），如果不加的话就是十六进制文件（.hex）。
- /m：表示备份为一个文件（这样方便日后 MTKWinFlash 的使用）。

2. 刷新 Firmware

而用 MTKFlash 刷新 Firmware 的命令格式是：mtkflash port w /b sso.bin，如图 1-25 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

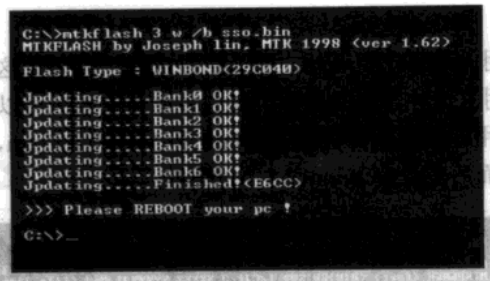


图 1-25

参数说明如下。

- port：表示是 IDE 端口号。
- w：代表写（刷新）。
- /b：代表以二进制文件（.bin）方式刷新，sso.bin 是要刷新的文件名，用户需根据下载的 Firmware 自己修改。

注意

需特别留意所下载的 Firmware 扩展名是.bin，还是.hex。如果是.hex 就千万不要加/b 这个参数。另外，如果下载到的 Firmware 是多个文件的话，请使用如下的格式来刷新：

```
mtkflash w /a0 /b bide00.bin
mtkflash w /a1 /b bide01.bin
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第2章 硬盘分区、格式化经典案例

硬盘分区、格式化是使用硬盘的一把“钥匙”，没有这把“钥匙”来开启，硬盘就只能“沉睡”着。选择合适的工具对自己的硬盘进行分区、格式化，是至关重要的。下面就来一一展示各款优秀的硬盘分区工具，以便读者更好地选择使用。

案例 07　使用 fdisk 对硬盘进行分区与格式化

fdisk 是传统的硬盘分区命令，fdisk 程序是 DOS 系统自带的分区软件，使用起来十分方便。在使用 fdisk 命令进行分区前，必须制作一个 DOS 启动盘，利用它进入纯 DOS 平台。下面以光盘启动盘为例介绍分区过程。

小知识

现在系统启动盘一般分为 3 种，分别是：软盘启动盘、光盘启动盘和 U 盘启动盘。软盘启动盘是大家最为熟悉的方式，且制作方法也比较简单；而光盘启动盘和 U 盘启动盘是现在比较流行的方式，在制作方面也是比较复杂的。大家可以根据自身的情况，选择制作需要的启动盘。

1. 从光盘启动进入纯 DOS 平台中

无论使用什么样的启动盘来启动系统，都需要对 CMOS 进行设置，将默认的从硬盘启动改为从软盘、光盘或者 U 盘启动，如图 2-1 所示。

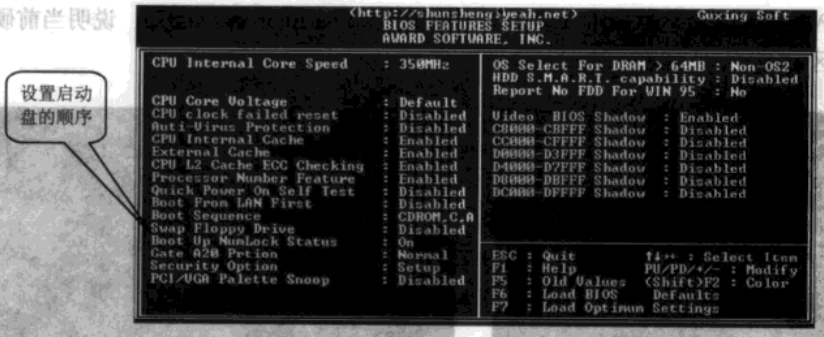


图 2-1

将 CMOS 设置为光盘启动后，将光盘放入光驱中启动计算机，会出现图 2-2 所示的界面。在 A:\>后输入 fdisk 并按回车键，即可进入图 2-3 所示的界面中。这里提示选择当前的分

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

区文件系统是 FAT32 格式还是 FAT16 格式，直接按回车键或按“Y”键则默认为以 FAT32 为当前文件系统。反之，则以 FAT16 为分区文件系统。



图 2-2



图 2-3

注意 FAT32 可以对 2GB 以上的硬盘进行分区，而 FAT16 则只能对最大 2GB 的硬盘进行分区，Windows 98 之后的操作系统分区文件一般都用 FAT32 格式。

然后，系统进入如图 2-4 所示的界面中，这是 fdisk 的设置主界面。

这里对图 2-4 中的 4 个选项分别进行说明。

注意

1．Create DOS partition or Logical DOS Drive：建立 DOS 主分区或扩展分区。

2．Set active Partition：用来设定开机的主分区，也是在分区后必须设置的一项。

3．Delete partition or Logical DOS Drive：用来删除已存在的分区。

4．Display partition information：显示当前的硬盘分区情况。

2．创建分区

创建分区之前首先要查看硬盘是否分过区，因为在购买机器时，销售商会对所购买的机器进行分区或安装 Windows 98/XP 等系统。查看方法为：在“Enter choice:”处输入 4，按回车键，如果进入如图 2-5 所示界面中（界面下方提示“No partition defined”），说明当前硬盘还没有进行分区。

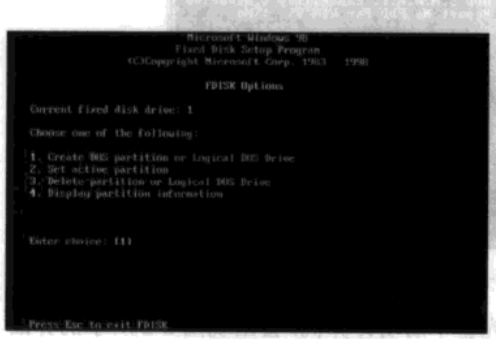


图 2-4



图 2-5

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（1）创建 DOS（主）分区

若出现图 2-5 所示的界面，则按键盘中的“Esc”键，回到图 2-4 所示的界面中。在“Enter choice:”处输入 1，按回车键，进入如图 2-6 所示的界面中，这时可参考规划好的分区方案对硬盘进行分区。

首先设置 DOS 主分区。在图 2-6 中的“Enter choice:”处输入 1，按回车键，进入如图 2-7 所示的界面，并开始对硬盘进行扫描。扫描完成后，进入如图 2-8 所示的界面。

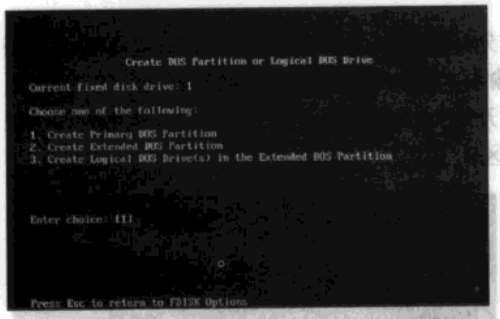


图 2-6

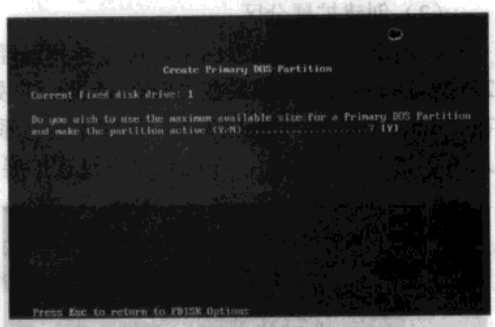


图 2-7

如果打算将硬盘分割成多个区，就是 D、E、F 或更多区的话，就要选择“NO”；反之，整个硬盘将会被直接分成一个主分区。

选择“N”选项后，就可以开始对 DOS 主分区进行容量划分，如图 2-9 所示。这里以当前硬盘容量是 16GB 为例，如果已经规划好硬盘的分区容量（如划分为 4 个分区：第 1 个分区为 Windows 98 系统盘，第 2 个分区为 Windows XP 系统盘或软件安装盘，第 3 个分区为软件安装盘或办公盘，第 4 个分区为资料和数据备份盘），就可以设置主分区的大小了。

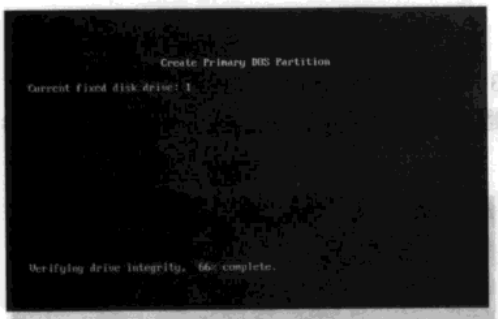


图 2-8

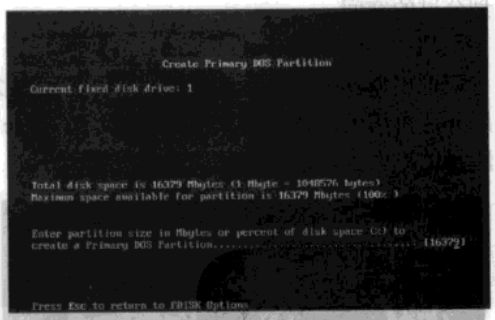


图 2-9

注意 这里划分的主分区也就是分区过后硬盘的“C:”盘，这个盘符中一般安装的是 Windows 98 系统，或者 Windows 2000/XP 系统。如果是前者，那么 C 盘符的容量如果设置得过大，就可能造成硬盘空间的浪费，一般 2GB 左右就可以了；如果是后者，那么 C 盘符的容量要设置得大一些，一般 5GB 左右就可以了。这只是笔者的意见，仅供参考。

如果确定主分区安装 Windows 98 系统，那么在“create a Primary DOS Partition.....:”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

处输入 2000，按回车键。

小知识 除了直接输入 2000 外，还可以利用百分比的形式来确定大小。如在“create a Primary DOS Partition.....”处输入 12%（即 2GB 约为硬盘总容量 16GB 的 12%）也可以的。不过，要以百分比的方式确定大小，必须在设置之前先算好当前设置容量占硬盘总大小的百分比，不然就会出现误差。

（2）创建扩展分区

在图 2-10 所示的界面中，可以看到已经划分好的主分区大小。接着按“Esc”键退到图 2-4 所示的界面中。然后在“Enter choice:”处输入 1，按回车键，进入图 2-6 所示的界面中。在“Enter choice:”处输入 2，按回车键，系统开始扫描，如图 2-11 所示。扫描完成后，进入图 2-12 所示的界面，在此界面中设置扩展分区。

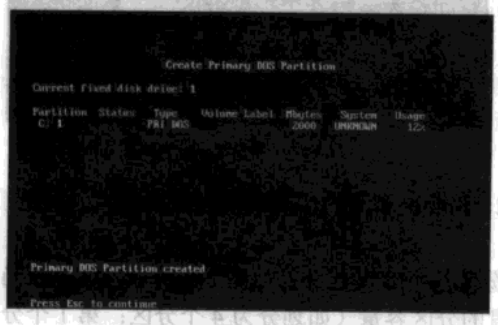


图 2-10

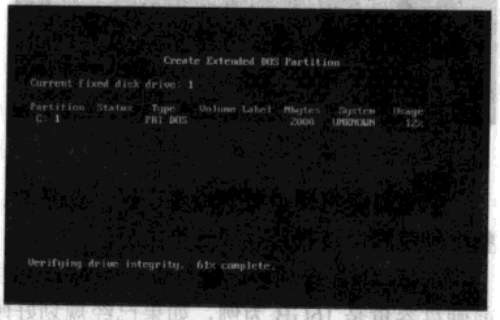


图 2-11

直接按回车键，不要修改默认设置。否则，改变了扩展分区的大小，会浪费硬盘上没有划分过的空间。

（3）创建逻辑分区

退出创建扩展分区的界面，即可显示图 2-13 所示的界面。在此界面中可以看到划分的扩展分区占用的硬盘空间大小。这时，按“Esc”键，开始进行扫描，扫描完成后，进入图 2-14 所示的界面中，创建具体的逻辑分区大小。

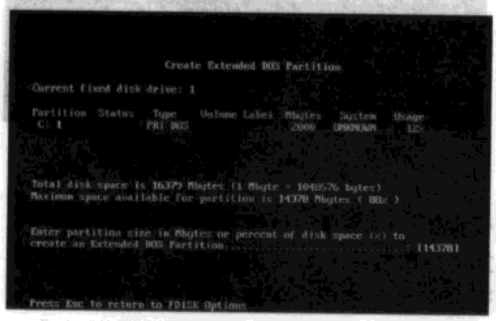


图 2-12

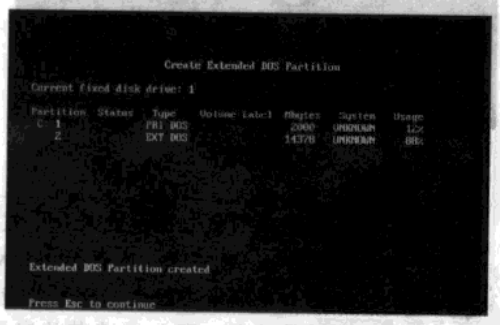


图 2-13

如第一个扩展分区（相当于 D 盘）是准备安装 Windows XP 系统盘或软件安装盘，可以将其设为 4GB 大小。然后，按回车键开始扫描，然后进入图 2-15 所示的界面，设置第二个

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

扩展分区的大小。如第二个扩展分区是软件安装盘或办公盘，这里可将其设为 5GB 大小。

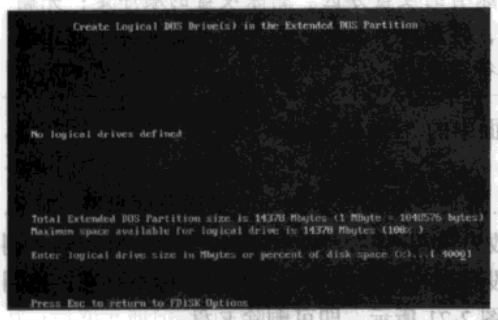


图 2-14

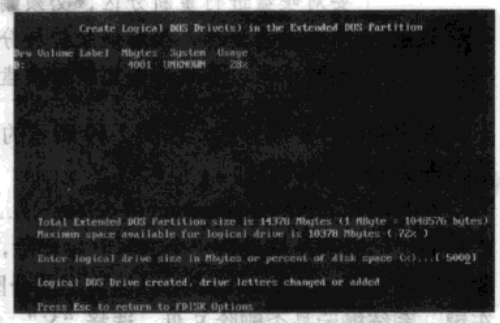


图 2-15

接着设置最后一个扩展分区，将硬盘剩下的空间设为最后一个扩展分区的大小即可，如图 2-16 所示。至此，硬盘分区划分完毕。

如果要查看当前硬盘的分区是否按照原定的规划进行，可以在图 2-4 所示的界面中，在“Enter choice：”处输入“4”，即可在图 2-17 所示的界面中看到当前主分区和扩展分区的情况。如果要进一步查看逻辑分区的大小，可直接按回车键进入图 2-18 所示的界面中查看扩展分区的情况。

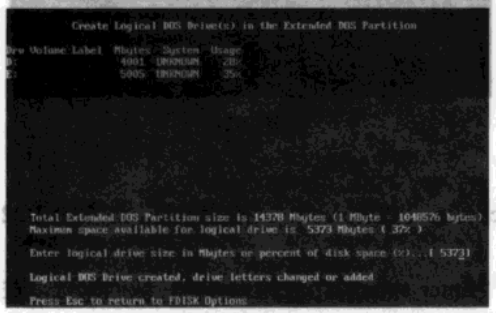


图 2-16

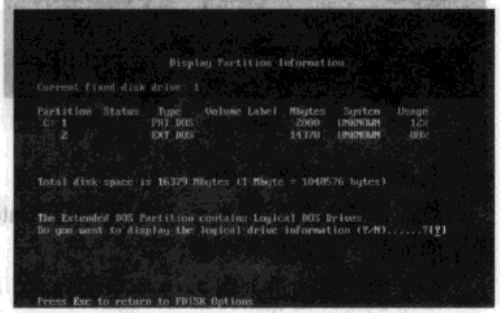


图 2-17

3. 删除分区

如果对当前的分区情况不满意，需重新划分，就需要先删除已经分好的区。在图 2-4 所示的界面中，在“Enter choice：”处输入“3”，回车，进入图 2-19 所示的界面中。

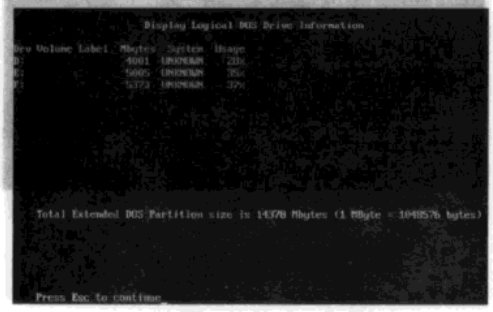


图 2-18

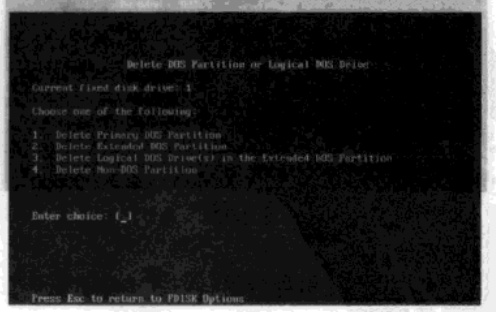


图 2-19

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

注意 要对硬盘进行重新分区，必须删除原有的硬盘分区。删除硬盘的顺序是：先删除各扩展分区，接着删除扩展分区，再删除主分区。如果顺序错误将不能正确删除分区，导致不能重新对硬盘进行分区。

首先删除各扩展分区，在图 2-19 所示的界面中的“Enter choice:”处输入 3，按回车键，进入图 2-20 所示的界面。

在“What drive do you want to delete.....”处输入要删除的扩展分区盘符，如 F、E 和 D。一般都是从最后一个分区开始删除，故先输入“F”，按回车键。系统会提示输入删除分区的卷标（Volume Label），因为当前分区没有进行高级格式化，所以卷标不存在。按回车键，系统提示是否删除 F 盘，选择“Y”，如图 2-21 所示，即可删除 F 盘。

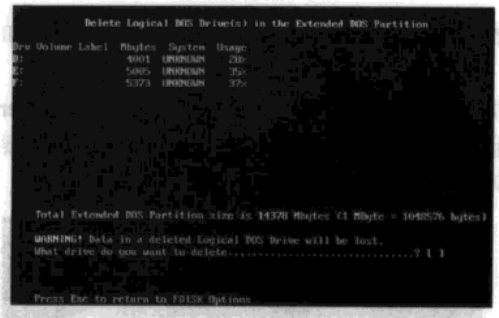


图 2-20

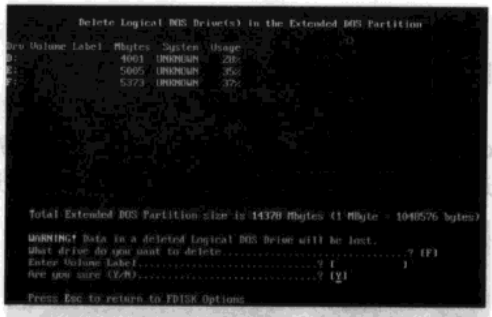


图 2-21

利用上述的方法，删除其他扩展分区。

然后，进入图 2-19 所示的界面，在“Enter choice:”处输入“2”，按回车键，进入图 2-22 所示的界面，删除扩展分区。

删除后，再次进入图 2-19 所示的界面，在“Enter choice:”处输入“1”，按回车键，进入图 2-23 所示的界面，删除主分区。这样，当前划分的所有分区都已经被删除了，然后按照上面介绍的分区方法重新对硬盘进行分区。

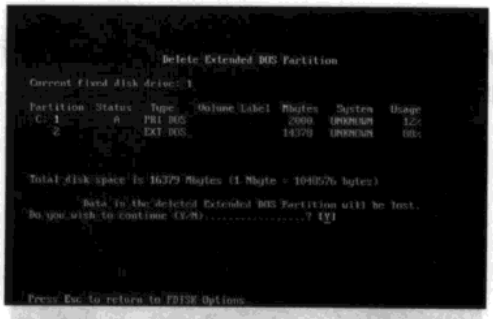


图 2-22

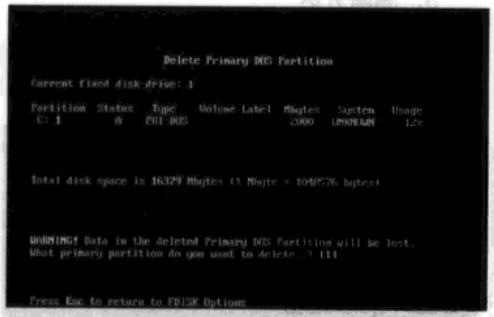


图 2-23

4. 设置主引导分区

如果当前的分区情况符合自己的需要，那么这时就需要设置硬盘主引导分区。在图 2-4

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

所示的界面的“Enter choice:”处输入“2”，按回车键，进入图 2-24 所示的界面。在“Enter the number of the partition you want to make active.....”处，输入要设置的主引导分区，一般以 C 盘作为硬盘的主引导分区，所以输入“1”（即选择 3C 盘），按回车键。这时在图 2-25 所示的界面中的“Status”下出现了一个“A”（即 Active），说明主引导分区已经设置。

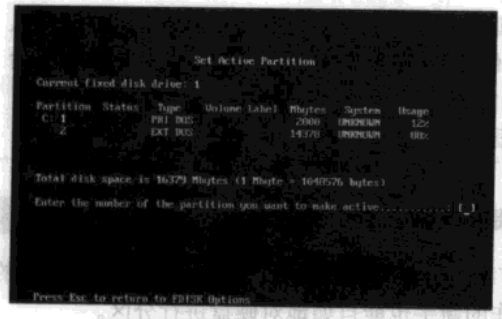


图 2-24

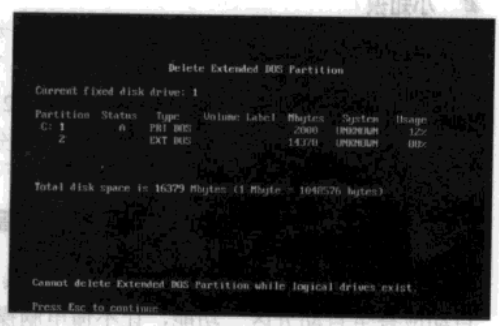


图 2-25

5. 格式化分区

通过上面的操作，硬盘分区已经完成，不过这时还不可以直接安装操作系统（如 Windows 98），必须退出 fdisk 分区界面，到纯 DOS 环境下对划分的分区进行格式化，然后才可以安装操作系统。

当按“Esc”键退出 fdisk 分区界面时，会弹出提示信息。这里不需要理会它，再次按“Esc”键进入纯 DOS 中。在“A:\>”后输入“format C:”，按回车键，即可开始对 C 盘进行高级格式化，如图 2-26 所示。对 C 盘的高级格式化完成后，出现提示信息，按回车键就可以建立 C 盘的卷标，此时 C 盘的卷标为“2C70-1601”，如图 2-27 所示。

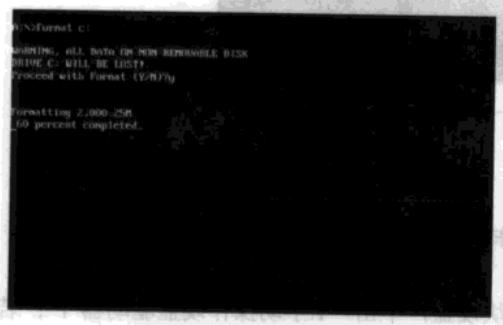


图 2-26

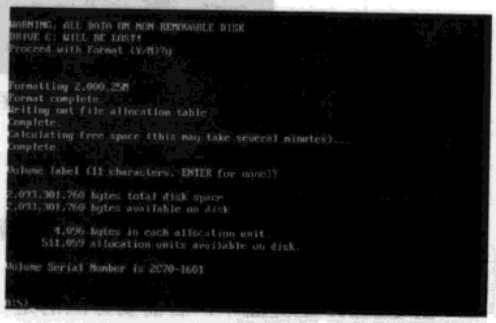


图 2-27

注意 上面已经提到过，如果在分区后没有进行高级格式化，则删除分区时就不需要输入卷标。但是在高级格式化后，如果要删除分区，就必须输入卷标。每一个分区的卷标都是在高级格式化后，系统自动产生的。

利用同样的操作，分别对其他分区进行高级格式化。完成这些后，就可以安装操作系统了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在分区的时侯都会输入数字，如想划分一个大小为 2GB 的分区，会输入“2000”或者“2048”。其实输入的这些数字所分出来的区在 Windows 下面都不会被认成整数的 2GB。想要使分出来的区的大小在 Windows 下被认成整数，可以通过以下这个公式计算。

小知识

$$Y=(X-1)*4+1024*X$$

其中 X 就是想要得到的整数分区的数值，单位为 GB。Y 是分区时应该输入的数字。如想得到 Windows 下的 2GB 整数空间，那么在分区时应该输入的数字为：$(2-1)\times4+1024\times2=2052$。

即在分区时输入 2052，则此分区在 Windows 下显示的大小为 2GB。

案例 08　使用 GDISK 对硬盘进行智能应答式分区与格式化

GDISK 是一款全中文硬盘分区工具，具有手工分区和智能化分区功能。此工具智能化的“自动应答全自动分区”功能，让不懂电脑操作的新手也能自如地对硬盘进行分区。

要使用 GDISK，先要将其拷入到 DOS 启动盘中。接着利用 DOS 启动盘进入 DOS 状态后，运行“GDISK”可执行文件就可以弹出 GDISK 的全中文界面，如图 2-28 所示。

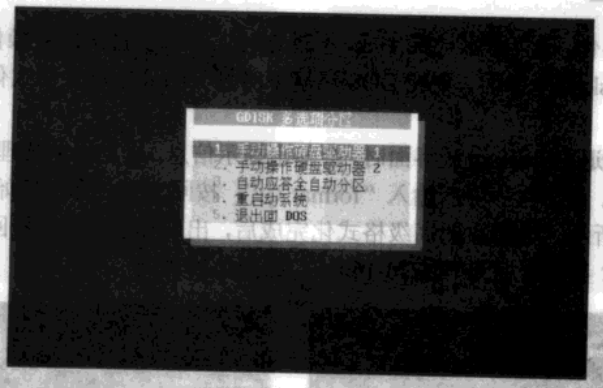


图 2-28

1. 手动对硬盘进行分区

先向大介绍如何利用 GDISK 的“手动操作硬盘驱动器”对硬盘进行分区。

（1）创建 DOS（主）分区

在 GDISK 主界面中，若需要分区的是 1 块硬盘，单击“1.手动操作硬盘驱动器 1”；若需要分区的是两块硬盘，单击“2.手动操作硬盘驱动器 2”。这里以 1 块硬盘为例。按回车键后进入“GDISK 分区主选项”窗口，如图 2-29 所示。

在图 2-29 中选中“创建 DOS 分区或 DOS 逻辑驱动器”，按回车键，进入“创建 DOS 分区或 DOS 逻辑驱动器”窗口，如图 2-30 所示。

这里首先要创建主 DOS 分区，所以在图 2-30 所示的窗口中选中“创建主 DOS 分区”选项，按回车键后，进入“创建主 DOS 分区”窗口中。按照窗口中提示的说明信息，在“1.请

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

指定你要创建主分区的大小”后，输入主分区的大小，如“02000”，如图 2-31 所示。输入完成后，将光标移动到“OK”按钮上，按回车键即可创建主 DOS 分区，如图 2-32 所示。

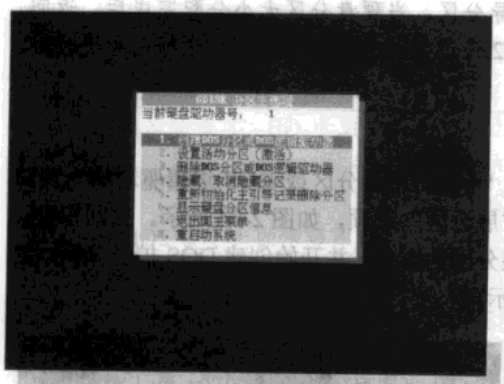


图 2-29

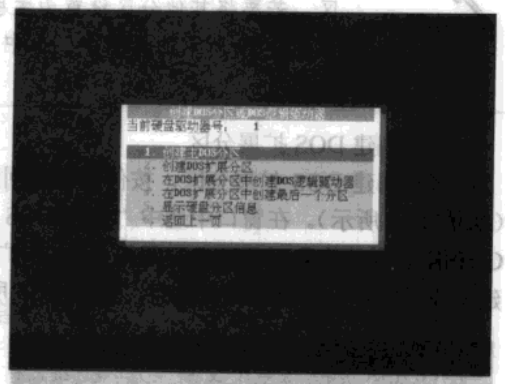


图 2-30

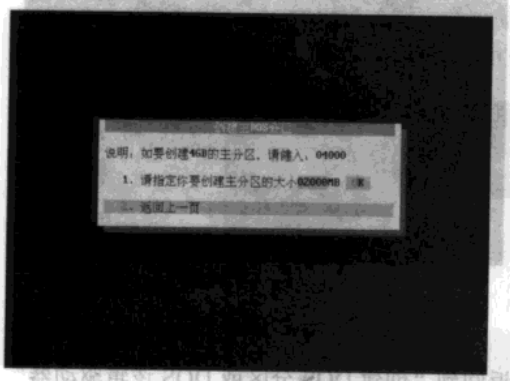


图 2-31

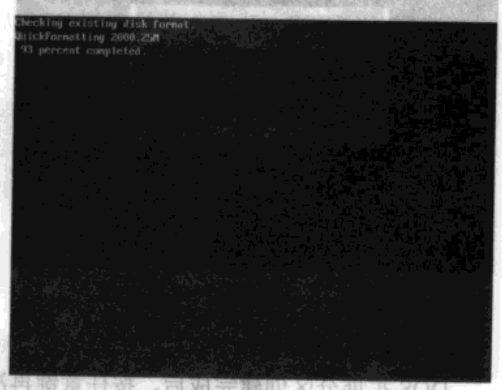


图 2-32

主 DOS 分区创建完成后，软件会自动给出主 DOS 分区的一些信息，如图 2-33 所示。可以按任意键继续进行 DOS 扩展分区的创建。

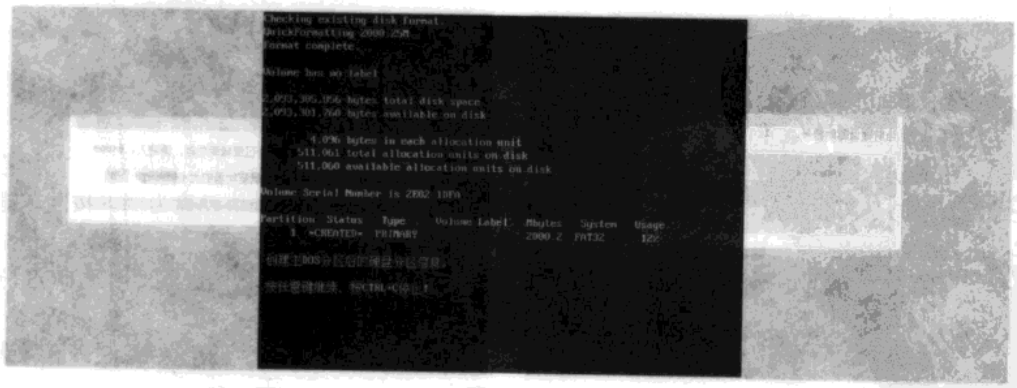


图 2-33

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

小知识

GDISK 在创建主 DOS 分区后，会自动将主 DOS 分区激活（在“Status”下显示“A”），作为主引导分区，而不需要用户再次激活 DOS 分区为主引导分区。若要将其他分区设置为主引导分区，当硬盘分区大小分配完成后，返回到图 2-29 所示的界面中，选中“2.设置活动分区（激活）”，根据向导进行设置即可。

（2）创建 DOS 扩展分区

接着创建 DOS 扩展分区，按任意键返回到“创建 DOS 分区或 DOS 逻辑驱动器”窗口（如图 2-30 所示）。在窗口中选中“创建 DOS 扩展分区”选项，如图 2-34 所示。按回车键，GDISK 会自动将剩下的硬盘空间作为 DOS 扩展分区的容量，并开始创建 DOS 扩展分区，创建完成后屏幕上会显示相关信息，如图 2-35 所示。

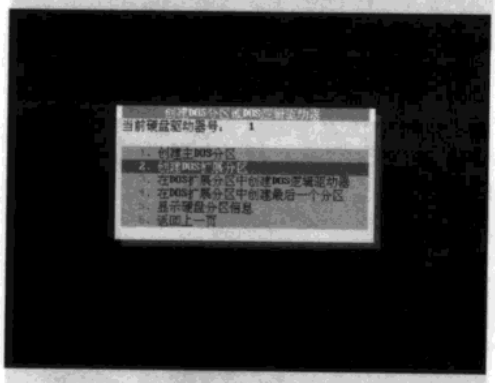


图 2-34

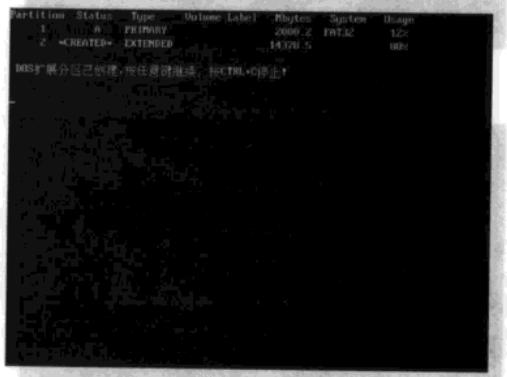


图 2-35

（3）创建 DOS 逻辑分区

DOS 扩展分区创建完成后，按任意键再次返回到“创建 DOS 分区或 DOS 逻辑驱动器”窗口。选中“在 DOS 扩展分区中创建 DOS 逻辑驱动器”选项，如图 2-36 所示。按回车键进入“在 DOS 扩展分区中创建 DOS 逻辑驱动器”窗口中，在“1.在扩展 DOS 分区中创建逻辑驱动器的大小”后输入第一个 DOS 逻辑分区的大小，如“04000”MB，如图 2-37 所示。

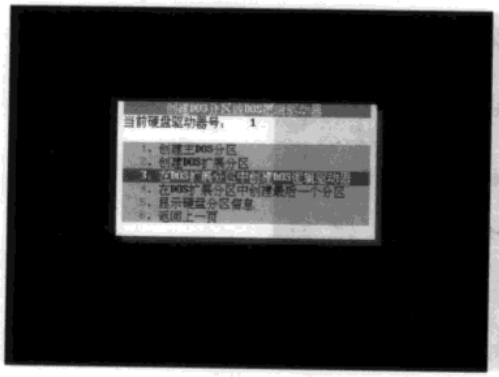


图 2-36

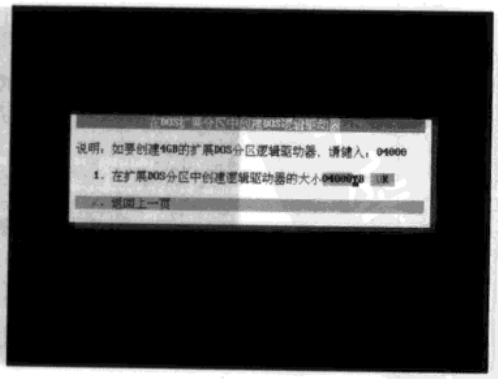


图 2-37

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

输入完成后，将光标移到“OK”上，按回车键即可创建第一个 DOS 逻辑分区，如图 2-38 所示。创建完成后，屏幕上会显示创建后的分区信息，如图 2-39 所示。

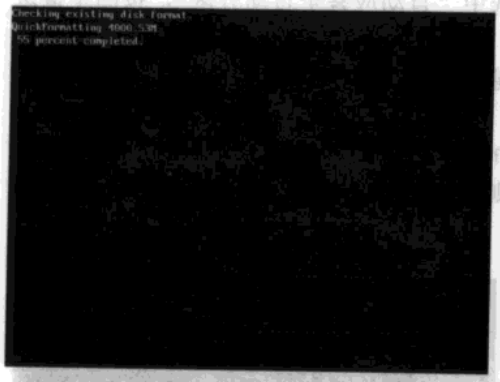


图 2-38

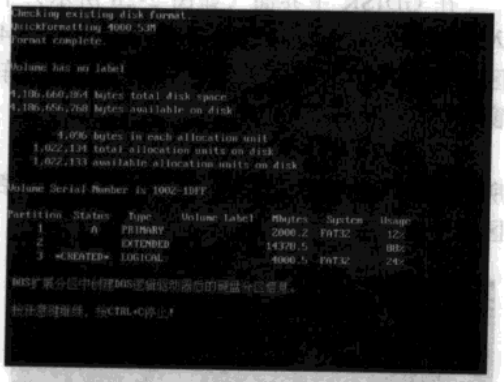


图 2-39

利用相同的方法，创建其他的 DOS 逻辑分区。直到创建最后一个 DOS 逻辑分区时，需要在“创建 DOS 分区或 DOS 逻辑驱动器”窗口中选中“在 DOS 扩展分区中创建最后一个分区”选项，如图 2-40 所示。这时 GDISK 会把所剩下的硬盘空间全部分配给最后一个逻辑分区，并开始创建。创建完成后，在窗口中显示所有分区信息，如图 2-41 所示。

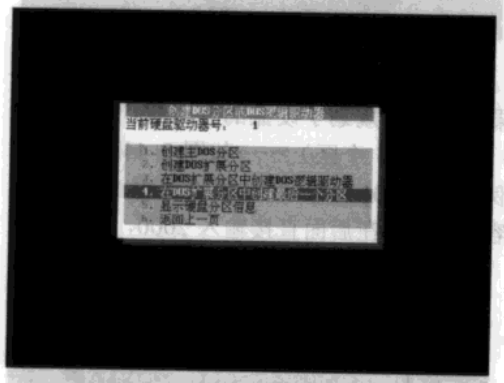


图 2-40



图 2-41

当最后一个 DOS 逻辑分区创建完成后，返回到“创建 DOS 分区或 DOS 逻辑驱动器”窗口中，选中“返回上一页”选项返回到 GDISK 主界面中，重新启动系统即可。

小知识 GDISK 在创建主 DOS 分区、DOS 扩展分区下的 DOS 逻辑分区后，都会自动对分区进行格式化。不需要重启系统后，在 DOS 提示符下利用 format 命令对各分区进行格式化。

2. 自动应答全自动分区

对电脑新手来说，可能会担心因误分区而导致硬盘分区划分不合理或损伤了硬盘。这里

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

可以利用 GDISK 提供的“自动应答全自动分区”功能，进行智能化应答式分区（就像学生提出问题老师解答问题一样）。

在 GDISK 主界面（如图 2-28 所示）中选中“自动应答全自动分区”，按回车键进入“自动应答全自动分区”窗口，如图 2-42 所示。默认状态下“1.自动应答全自动分区”选项是被选中的，这时可以直接按回车键进入“Gdisk 定制自动应答文件生成器”窗口中。

系统提示“请确认硬盘是否已经有分区，如有请输入大写 Y，否则输入 N”，如图 2-43 所示。若当前硬盘已经有分区，按 Y”键；否则按“N”键。接着按回车键，进入下一个分区应答提示中。



图 2-42

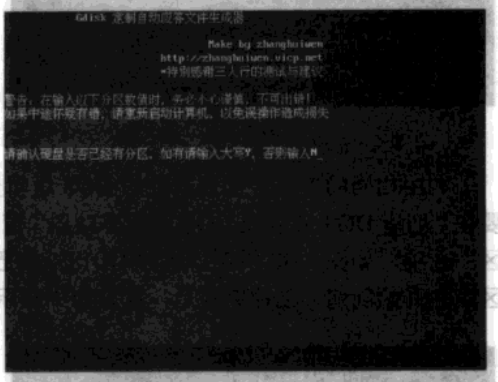


图 2-43

这时提示“请问您要分几个区呢？”，如果用户已经规划了硬盘的分区数，可以在后面直接输入分区数，如 4（表示分 4 个区）、5（表示分 5 个区）……如图 2-44 所示。接着按回车键，系统提示“首个分区要几 G 呢[例 2G=2000]:？”，在这里设置主 DOS 分区的容量大小。如果为主 DOS 分区分配 2GB 的容量，可以在后面直接输入 2000，如图 2-45 所示。

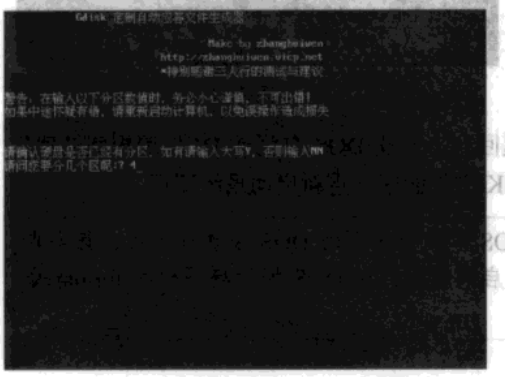


图 2-44



图 2-45

再按回车键，为第 2 个分区和第 3 个分区设置大小，如图 2-46 和图 2-47 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

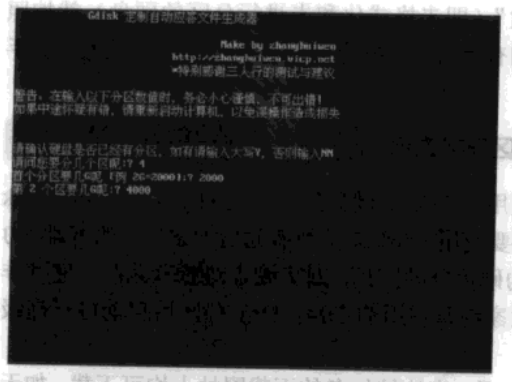


图 2-46

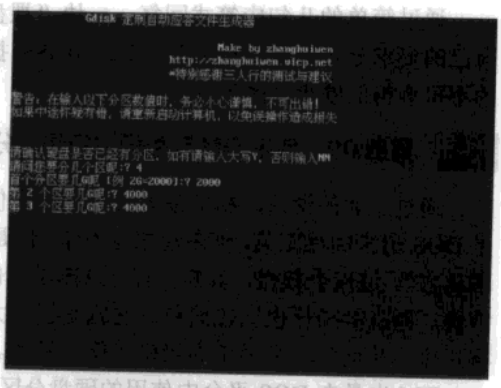


图 2-47

当第 3 个分区的大小设置完成后，GDISK 就开始对照上面的应答回复结果对硬盘进行分区。先创建主 DOS 分区，如图 2-48 所示；接着创建 DOS 扩展分区，如图 2-49 所示；最后创建 DOS 扩展分区中的 DOS 逻辑分区，如图 2-50 所示。

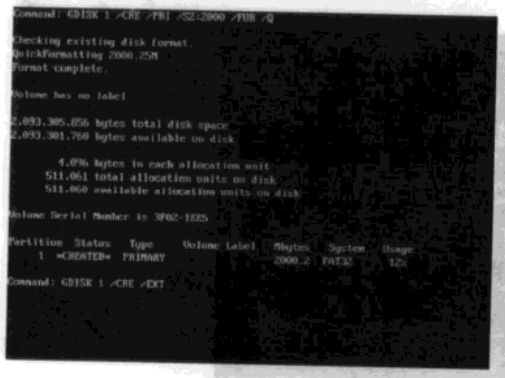


图 2-48

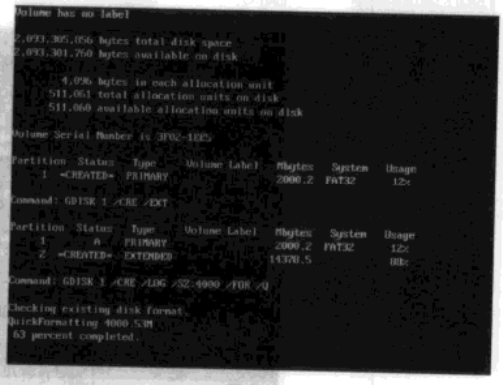


图 2-49

分区创建完成后，窗口中会显示各分区信息，如图 2-51 所示。

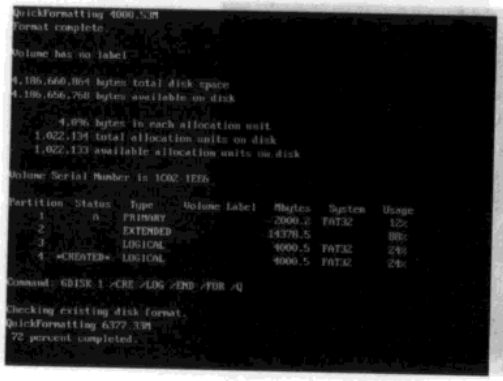


图 2-50

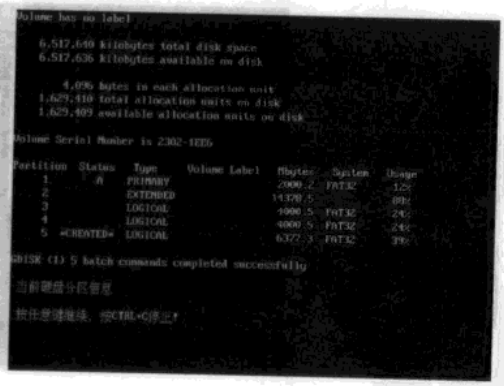


图 2-51

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

通过简单的几句应答式回复，一块“裸盘”（即未格式化和未进行分区的硬盘）就按照自己的要求分好区了，操作很简单。GDISK 拥有“自动应答全自动分区”功能，是电脑新手的不可多得的硬盘分区工具。

案例 09　使用 DM 对硬盘进行快速分区与格式化

通过上面的学习，相信读者已经掌握了使用 Fdisk 对硬盘进行分区的方法。虽然 Fdisk 是 DOS 自带的小工具，使用起来也不错，但是要使用 Fdisk 对大硬盘进行分区，它就有点“力不从心”，速度会很慢。其实，有一款挺不错的硬盘分区工具，对大硬盘进行分区时，速度非常快，而且其操作也比较简单。它就是现在大家经常使用的 DM，DM 分区后自动进行高级格式化，从而省去了手工高级格式化的操作。

DM 也是在 DOS 平台中使用的硬盘分区工具，在比较知名的下载网站上均可下载，如天空软件站、华军软件园等。下面就来看看如何使用 DM 对硬盘进行分区。

首先，利用启动盘启动电脑，进入纯 DOS。在相应的目录中找到解压后的 DM 目录，运行 DM，进入如图 2-52 所示的界面，此界面是 DM 说明窗口。按任意键即可进入 DM 的主界面，如图 2-53 所示。

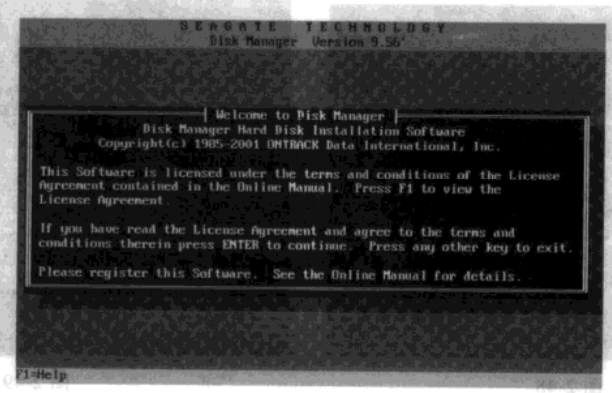


图 2-52

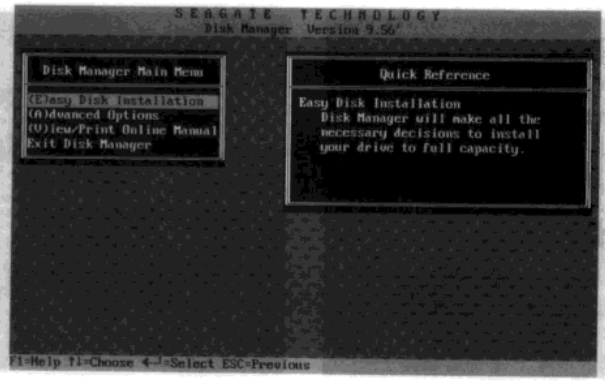


图 2-53

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在主界面中，有 4 个主菜单，这里对其进行简单的介绍。

- E asy Disk Installation：此菜单的主要功能是对硬盘进行分区。
- A dvanced Options：此菜单的主要功能是对硬盘进行高级分区。
- V iew/Print Online Manual：此菜单的主要功能是提供一些帮助信息和常用硬盘的主/从盘跳线设置图。
- Exit Disk Manager：此菜单的主要功能是退出 DM。

注意 主菜单下的前 3 个选项的首个字母 E、A、V 都被括弧括起来了，即表示可直接按 E 键、A 键、V 键进入相应的菜单。

下面看看 DM 是如何对硬盘进行分区的。要按照自己规划的大小来分区，这里不能选择“E asy Disk Installation”选项菜单来进行分区。否则，会把当前硬盘划分为一个分区。

这里选择“A dvanced Options（高级分区）”选项菜单来进行分区。选择后，按回车进入“Advanced Options”界面中，如图 2-54 所示。

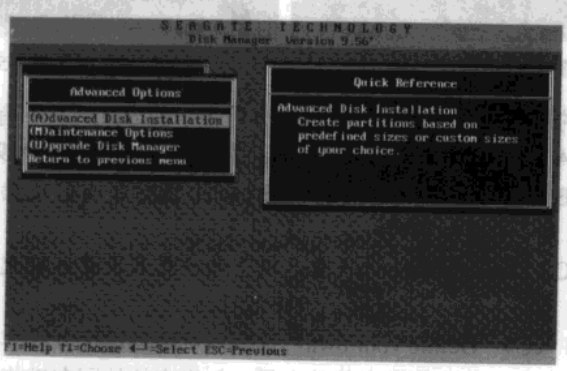


图 2-54

选择默认的“A dvanced Disk Installation”选项，这是分区的第一步操作。接着，按回车进入如图 2-31 所示界面中。此界面中显示当前硬盘信息，如果是多个硬盘，则在图 2-55 所示界面右边的“Drive List”中显示多个硬盘信息。DM 可以有选择地对某一个硬盘进行分区，如果当前机器只有一个硬盘，那么选择默认的选项，按回车键进入如图 2-56 所示的界面。

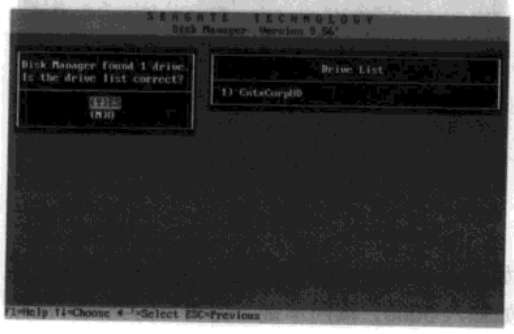


图 2-55

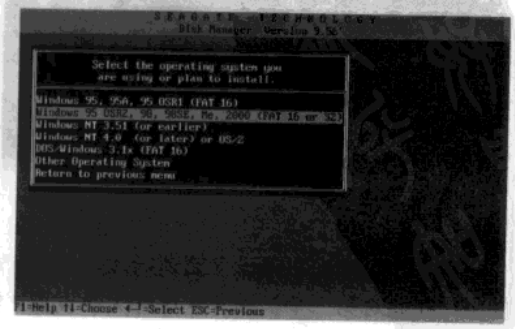


图 2-56

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在图 2-56 所示的界面中，提示选择当前硬盘的文件格式，默认是“Windows 95，95A，95 OSR1（FAT16）”选项。因为此选项最多支持 2GB 的容量，所以这里选择“Windows 95 OSR2，98，98SE，Me，2000（FAT 16 or 32）”选项，接着按回车键进入如图 2-57 所示的界面。

该界面提示是否使用 FAT32 文件系统，如果是，选择默认的“（Y）ES”选项；反之，选择“（N）O”选项。按回车键进入如图 2-58 所示的界面。

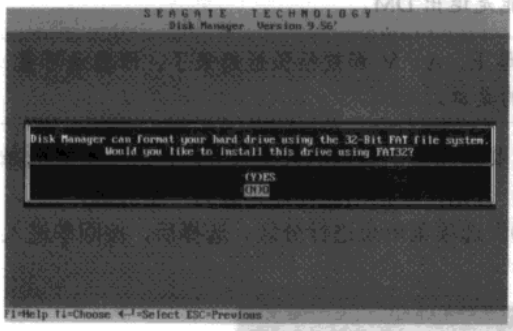


图 2-57



图 2-58

在图 2-58 所示的界面中，主要是选择设置分区大小的方式。其中有 3 个选项。

- OPTION（A）1 partition with 17.17GB：表示将当前硬盘整块设为一个分区。
- OPTION（B）4 partitions with 4.293GB each：表示将当前硬盘分为 4 个分区，而且每一个分区大小都是相同的。
- OPTION（C）Define your own：表示以手动方式来设置当前硬盘的分区和相对应的分区大小。

选择“OPTION （C） Define your own”选项，对硬盘进行分区。按回车键进入图 2-59 所示的界面中。此界面显示了当前硬盘的总容量，如果直接按回车键将把当前硬盘作为一个分区，所以这里必须自行设置，而第一次进行设置的是 C 盘，也就是主引导盘。如输入 2000，按回车键进入图 2-60 所示自行界面。

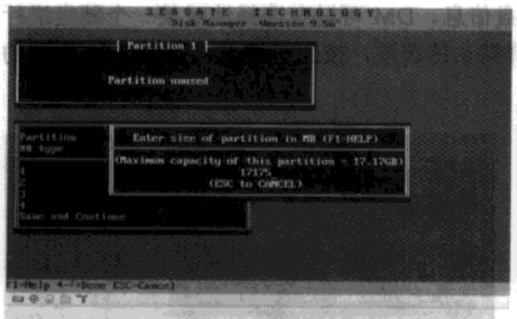


图 2-59

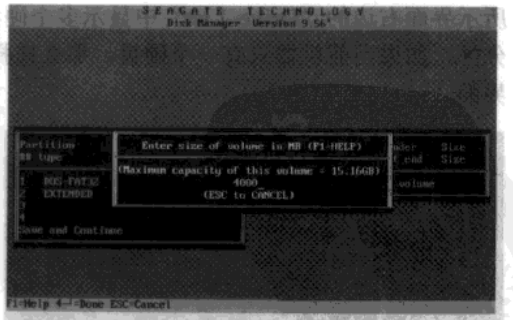


图 2-60

在此对第一个扩展分区盘进行大小设置，如输入 4000。按回车键进入图 2-61 所示的界面中。在此对第二个扩展分区进行大小设置，如输入 5000。按回车键，把剩下的空间分配给最后一个扩展分区，如图 2-62 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

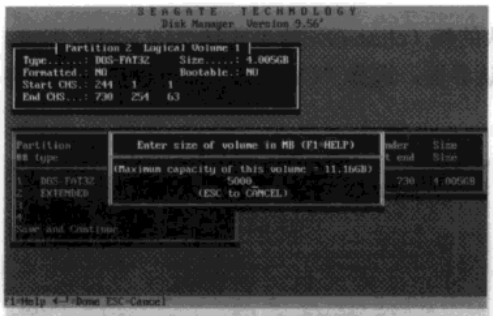


图 2-61

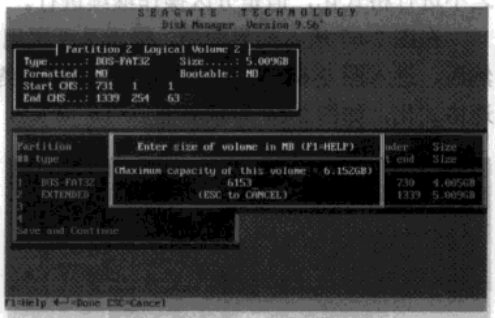


图 2-62

硬盘分区和分区大小设置完成后，即可在图 2-63 所示的界面中看到主分区和扩展分区的相关信息。如果对分区不满意，按“Esc”键退出分区大小设置窗口，弹出图 2-64 所示的界面。这里选择“（N）O”，按回车键即可回到图 2-58 所示的界面中，然后利用上面用的方法重新对硬盘进行分区。

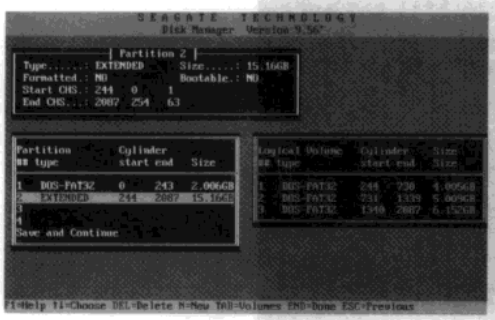


图 2-63

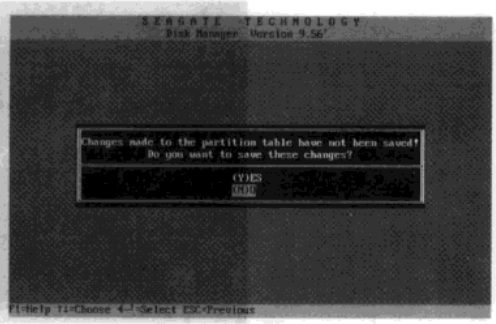


图 2-64

如果确定硬盘分区大小跟规划方案一样，那么就可以在图 2-63 所示的界面中选中“Save and Continue”选项，按回车键，弹出如图 2-65 所示界面。再次确认分区设置，可按“Alt+C”组合键将进入图 2-66 所示的界面。否则，按任意键回到主菜单。

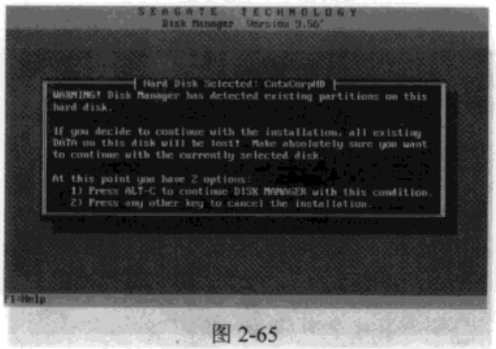


图 2-65

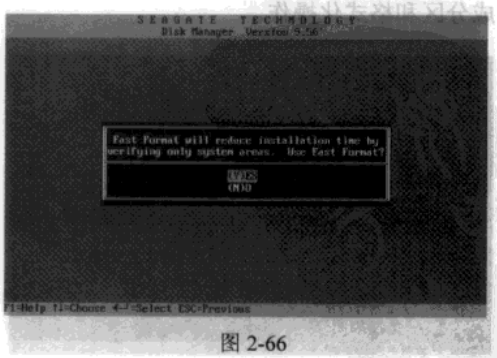


图 2-66

图 2-66 所示的界面提示是否进行快速格式化，选择“（Y）ES”则进行快速格式化；反

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

之不进行格式化，但是分区操作继续进行。

在图 2-67 所示的界面中，提示是否采用默认的簇（cluster），这里选择“（Y）ES”即可。然后，进入图 2-68 所示的界面中，这是最终确认界面，选择“（Y）ES”即可进行分区和快速格式化，如图 2-69 所示界面。



图 2-67

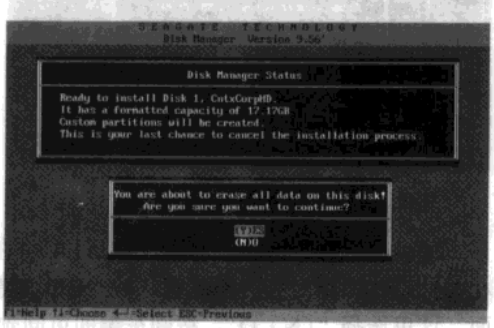


图 2-68

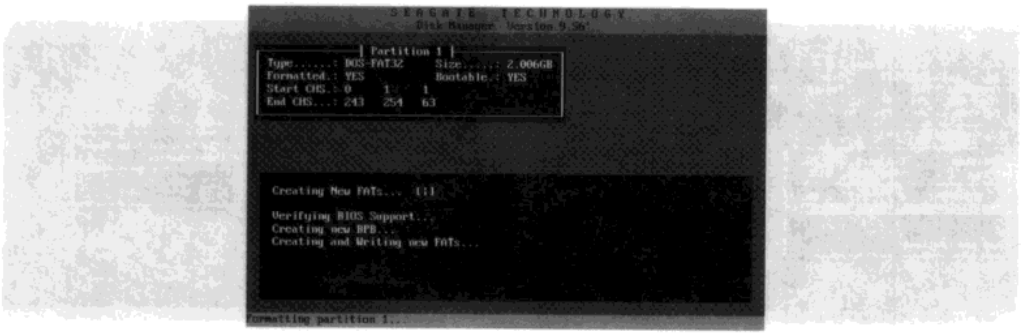


图 2-69

使用 DM 对大硬盘进行分区和格式化的速度非常快，当分区和快速格式化完成后，弹出图 2-70 所示的界面。提示分区和快速格式化操作已经完成，按任意键进入图 2-71 所示的界面，按照提示按主机面板上的“RESET”键或按“Ctrl+Alt+Del”组合键重新启动计算机，完成分区和格式化操作。

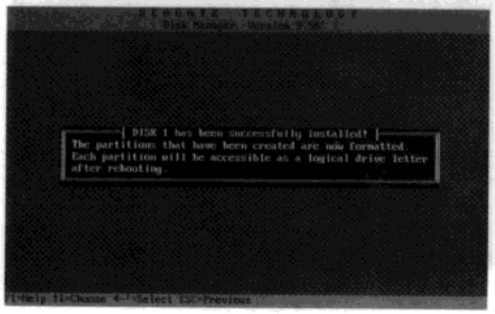


图 2-70

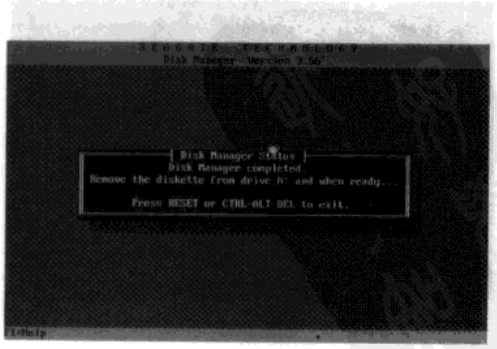


图 2-71

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

重新启动系统后，硬盘已经按照规划的方案完成分区和格式化。这时可以安装操作系统了。

小知识 虽然 DM 提示可以使用热启动的方式（即按“Ctrl+Alt+Del”组合键）重新启动系统，但是建议采用冷启动，也就是按主机面板上的“RESET”重新启动。

DM 的功能并不只有分区一项，其实它还有强大的低级格式化功能。大家都知道，对硬盘进行低级格式化会减少硬盘的寿命，但是使用 DM 对硬盘进行低级格式化，能最大限度地保护硬盘，并且对物理坏道进行修复，使快要“报废”的硬盘“起死回生”。

案例 10 使用 PartitionMagic 对硬盘进行分区与格式化

PM 是 Partition Magic 的缩写，中文名字叫磁盘分区魔术师。它是一款非常优秀的磁盘分区管理软件，而且全面支持 Windows 平台。它的主要功能包括：可实现硬盘动态分区和无损分区，支持大容量硬盘，可以轻松实现 FAT 和 FAT32、NTFS 系统间相互转换，同时还能非常方便地实现分区的拆分、删除、修改，并且还可以实现多 C 盘引导等。

PM 与 DM 最大的区别在于：它是向导化的操作，只需要配合鼠标就可以方便地完成硬盘的分区操作。下面来看看 PM 是如何对硬盘进行分区操作的。

注意 这里需要提醒读者，PM 虽然支持 Windows 平台，但是要对裸盘进行分区，必须在 DOS 下进行。而且 PM 在 DOS 下只提供英文版，在 Windows 平台中可以提供简体中文版。

首先，利用启动盘进入纯 DOS，放入带有 PM 工具的光盘，进入 PM 所在目录，再执行 pqmagic.exe 文件，即可打开 PM 的主界面。当 PM 执行时，已经开始对硬盘进行扫描和检测，并显示当前硬盘的容量，如图 2-72 所示。

所有未使用的空间以灰色显示出来，现在来看如何使用 PM 建立分区。因 PM 支持鼠标的使用，所以只要通过鼠标就可完成操作。

这里先用 PM 创建主分区。单击工具栏上的“C:”按钮，或单击“Operations”菜单中的“Create”选项，弹出如图 2-73 所示的界面。

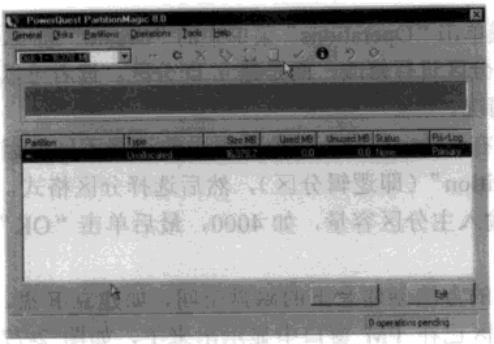


图 2-72

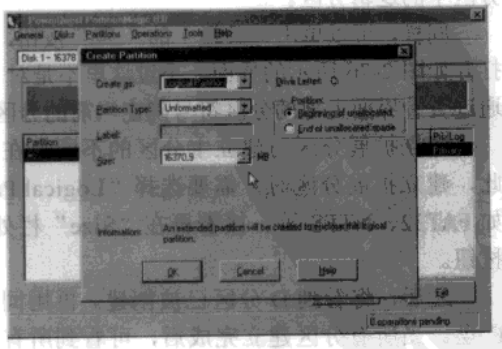


图 2-73

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

小知识 可以将鼠标移至灰色条处，单击鼠标右键，在弹出的快捷菜单中选择“Create”选项，也能打开如图 2-73 所示的界面。

单击“Create as”下拉列表右边的小三角按钮选择分区类型，这里选择 Primary Parition（即主分区），接着在“Partition Type”下拉列表中选择当前分区的文件系统（分区格式）。

注意 与 Fdisk 和 DM 不同的是，PM 除了可建立 FAT 格式分区外，还可建立其他分区格式，如 NTFS、Swap 等。

在“Label”栏处输入分区卷标，一般情况下不需要输入，PM 在分区后会自动生成相应的分区卷标；在“Size”栏处输入主分区容量，单位是 MB，如输入 2000，如图 2-74 所示。

当所有设置完成后，单击“OK”按钮，即可看到主分区 C 盘被建立了，如图 2-75 所示。

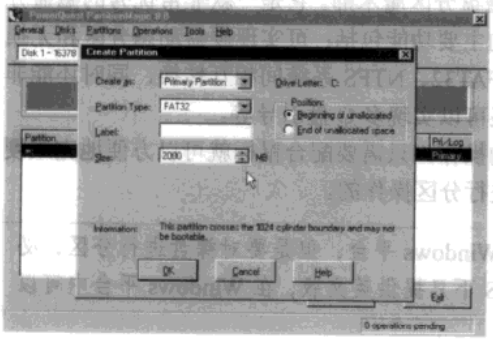


图 2-74

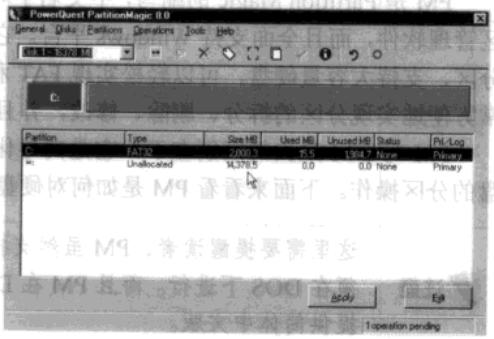


图 2-75

注意 这里看到的主分区 C 只是 PM 以模拟形式展现出来的，其实并没有真正的分区。只有等扩展分区的模拟形式建立后，PM 才会根据模拟形式把硬盘划分成主分区和扩展分区。

这样就建立了主分区 C，在硬盘中最多可以建立 4 个主分区。如果需要，还可以在 PM 中通过上面的方法继续建立。不过一般情况下，只需要建立一个主分区。下面就来建立扩展分区中的逻辑分区。

同样，可以单击工具栏上的“C:”按钮，或单击“Operations”菜单中的“Create”选项，打开如图 2-76 所示的界面。不过这里不是对 C 分区进行修改，而是建立 D 分区。读者可以通过查看界面上部的分区符号确定当前的分区情况。

建立扩展分区与建立主分区的不同点在于在“Create as”下拉菜单中的选择不同。因此，建立扩展分区时，需要选择“Logical Partition”（即逻辑分区），然后选择分区格式，如 FAT32、NTFS 等。接着再在“Size”栏处输入主分区容量，如 4000，最后单击“OK”按钮。

之后，将看到 D 分区已被创建。再用同样的方法创建余下的磁盘空间，如建立 E 盘、F 盘。当所有分区建立完成后，可看到所有分区已在 PM 窗口中显示出来了，如图 2-77 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

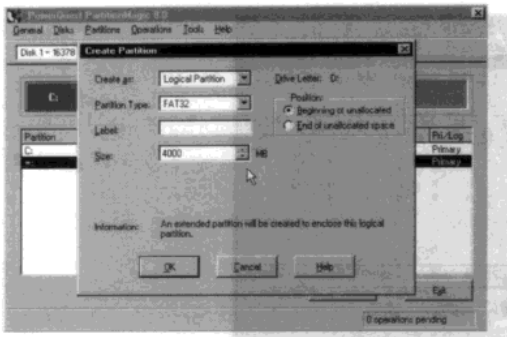


图 2-76

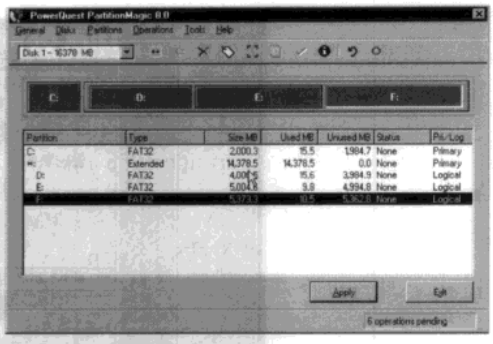


图 2-77

分区建立完成后，还可以对创建的模拟形式进行调整。确定创建的模拟形式已经满足要求，单击如图 2-77 所示界面中的“Apply”按钮，弹出图 2-78 所示的界面。提示是否确认分区大小，确认则单击“Yes”按钮，PM 开始按照设置的分区大小进行创建。

注意 PM 跟 DM 一样，在创建分区的同时已经对分区进行了高级格式化。

PM 创建分区也同样需要重启计算机设置才能生效，当创建完成后退出时，就会提示重启计算机，如图 2-79 所示。

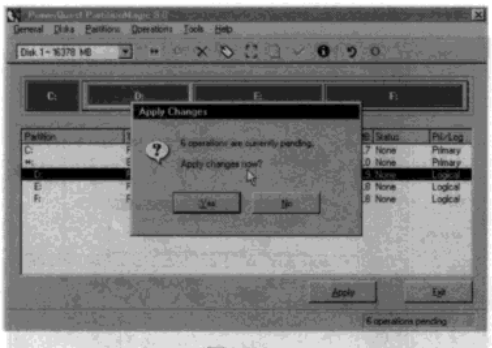


图 2-78

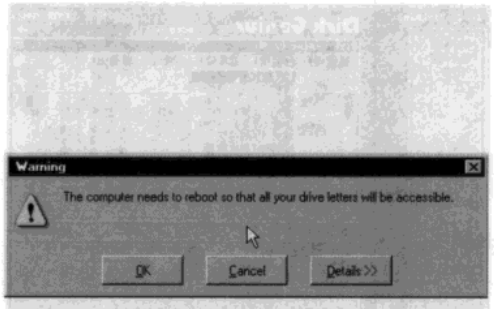


图 2-79

重新启动计算机后，PM 就完成了硬盘的分区操作。其实，PM 的功能远远不止这些，它还具有格式转换、在无损数据的情况下调整分区容量等（这些操作方法将在以后的内容中介绍）。

案例 11 使用 Disk Genius 对硬盘进行分区与格式化

Disk Genius 是一款优秀的国产磁盘分区工具，全面支持 FAT、FAT32、NTFS 分区格式，还可以自由地在这些分区格式之间进行转换。这款工具具有基于纯 DOS 平台的简体中文界面，且软件的大小只有 149KB。

将 Disk Genius 拷入启动盘中，通过启动盘进入 DOS，运行 diskgen 即可进入“Disk Genius”主界面，如图 2-80 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 2-80

1．新建主分区

在“Disk Genius”主界面中，单击“分区”→“新建分区”（如图 2-81 所示）选项，弹出“新建主分区”对话框。此时会要求输入新分区的大小，这里输入 2000（即 2GB），如图 2-82 所示。

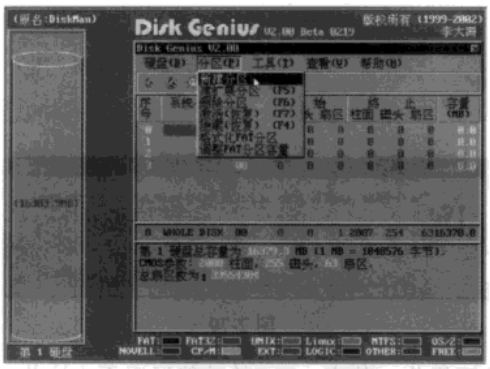


图 2-81

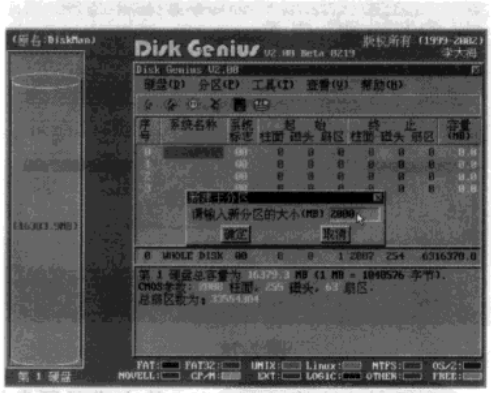


图 2-82

主分区的大小确定后，单击“确定”按钮弹出“要建立 DOS FAT 分区吗？”提示对话框，如图 2-83 所示。若选择“是”那么软件会根据刚才输入的分区大小进行设置，此分区大小若小于 640MB 该分区将被自动设为 FAT16 格式，否则会自动设为 FAT32 格式。若选择“否”，软件将会提示手动填写一个系统标志，并在右边窗体的下部给出系统标志的列表供读者参考。如将主分区设置为 NTFS 格式，只需要在“请输入系统标志”栏中输入“07”（可以通过下面的“系统标志”获得对应的标志编号），如图 2-84 所示。

主分区的格式确定后，主分区也就创建完成（主分区就是硬盘上的 C 盘）了。在界面的左边的圆柱中以蓝色显示的那一段即主分区，如图 2-85 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 2-83

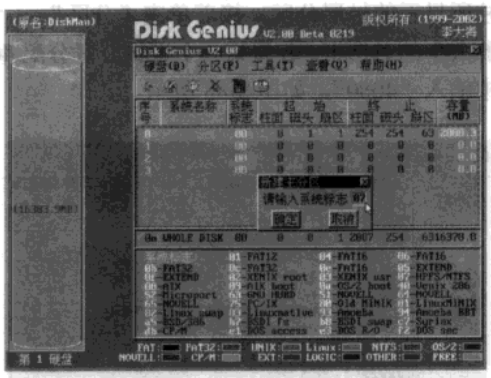


图 2-84



图 2-85

注意 这里最好将主分区的分区格式设置为 FAT32 分区格式，方便安装 Windows 操作系统；反之，设置为 NTFS 分区格式，在 DOS 下不能识别，无法安装 Windows 操作系统。

2. 新建扩展分区

当主分区建立完成后，接着就需要创建扩展分区。只有建立了扩展分区，才可以建立逻辑分区，即 D、E、F 等盘。

在“Disk Genius”界面中，选中左边圆柱没有使用的那一段空间，接着单击“分区”→“建扩展分区”选项，弹出“新建扩展分区”对话框。通常情况下应该将所有剩余的空间都建立为扩展分区，所以这里可以直接单击“确定”按钮，如图 2-86 所示。

扩展分区建立完成后，在左边的圆柱中以绿色显示出来，如图 2-87 所示。

3. 新建逻辑分区

扩展分区建好后，接下来创建扩展分区下的逻辑分区，即 D、E、F 等盘。先选中左边圆

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

柱所显示的扩展分区，接着单击“分区”→“新建分区”选项，弹出提示输入新建逻辑分区的大小的对话框。若为第一个逻辑分区分配 4000 大小，即可在“请输入新分区的大小（MB）”中输入“4000”，如图 2-88 所示。

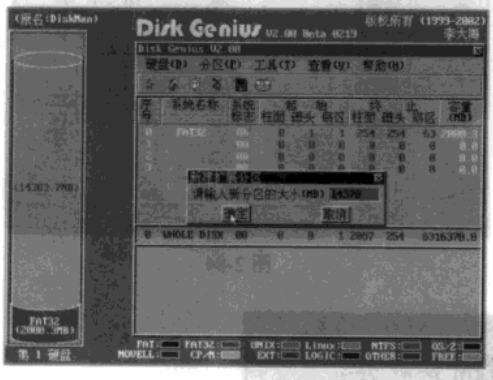


图 2-86

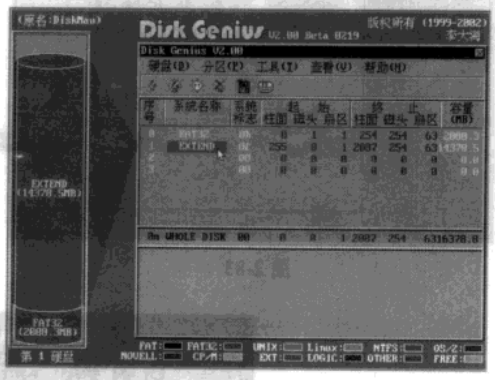


图 2-87

单击“确定”按钮，弹出为该逻辑分区建立分区格式的界面。这里单击“是”按钮，以默认的 FAT32 作为逻辑分区格式。这样，第一个逻辑分区就建立完成，即硬盘的 D 盘，如图 2-89 所示。

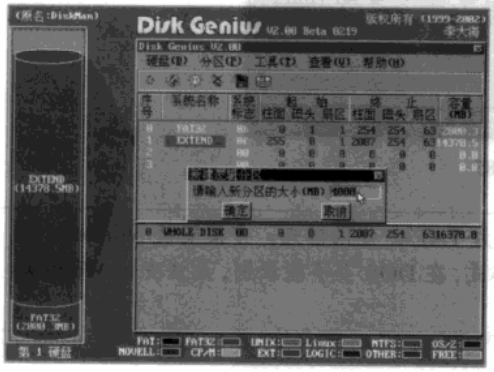


图 2-88

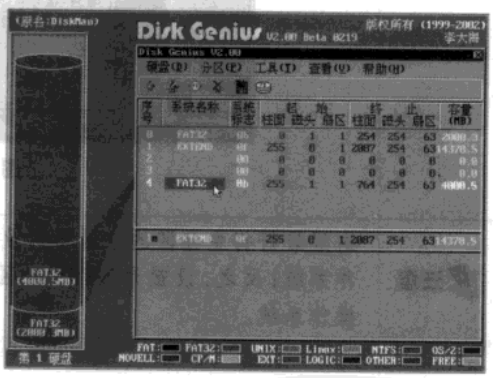


图 2-89

建立了第一个逻辑分区之后，可以按照建立第一个逻辑分区的方法在剩余的未分配的扩展分区上继续建立其他逻辑分区，也就是相应的 E、F 等盘，直到所有的空间全部分配完成，如图 2-90 所示。

4．删除分区

若在分区后，感觉有的盘分配的空间有点小了，不能满足实际的需求。这时可以删除分区，重新分配分区大小。

先选中要删除的分区，接着单击“分区”→“删除分区”选项，弹出“确实要删除此分区吗？”提示对话框，如图 2-91 所示。单击“删除”按钮即可删除选中的分区。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

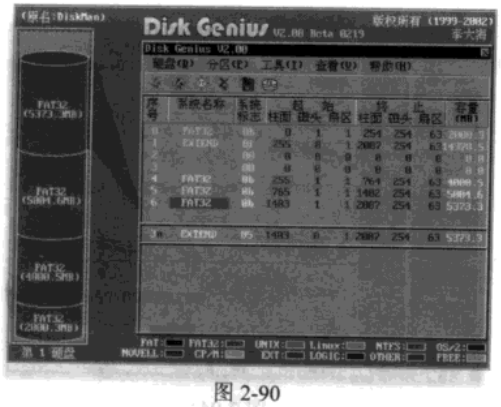


图 2-90

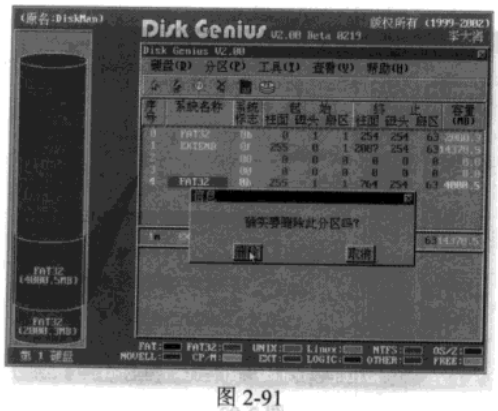


图 2-91

5. 设置主引导分区

硬盘的分区大小都分配完成后，就需要设置主引导分区，也就是引导系统启动的分区。通常都以主分区（即 C 盘）作为主引导分区，接下来就需要激活它。

选中主分区，单击“分区”→“激活（恢复）”选项，即可激活主分区。激活之后，该分区的“系统名称”下以红色字体显示，如图 2-92 所示。

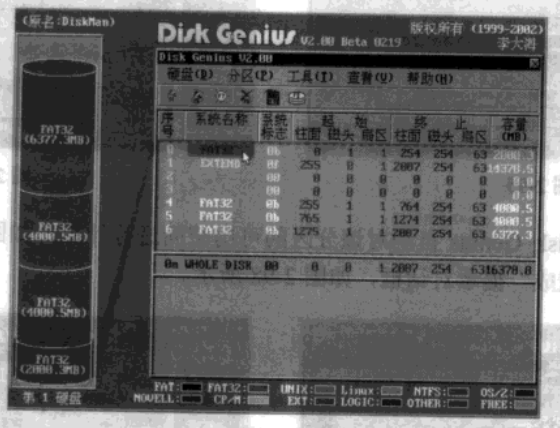


图 2-92

6. 分区格式化与存盘更新分区表

通过上面的操作，硬盘的整个分区设置就算完成了。接下来就需要对各分区进行格式化，格式化完成后，一个完整的硬盘分区操作才算完成。

先选中主分区，单击“分区”→“格式化 FAT 分区”选项，弹出“设置簇大小”对话框，如图 2-93 所示。直接单击“确定”按钮，即可进行分区格式化操作，如图 2-94 所示。

格式化结束后，会自动弹出一个对话框，提示用户对硬盘进行检测，如图 2-95 所示。如果用户不放心自己的硬盘状况，可以单击“检测”按钮进行检测，如图 2-96 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

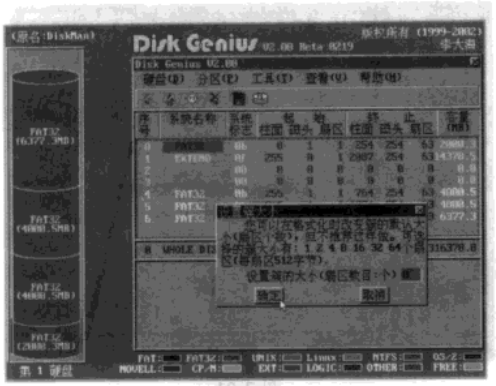


图 2-93

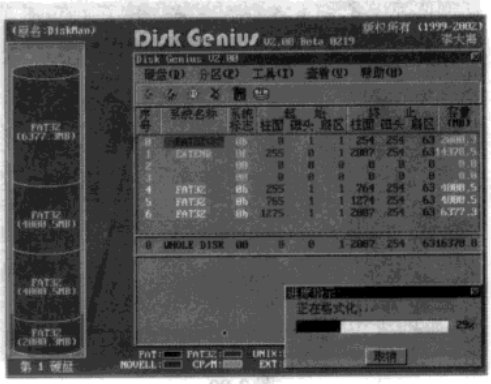


图 2-94

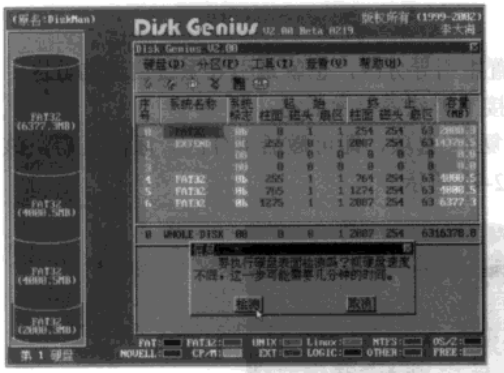


图 2-95

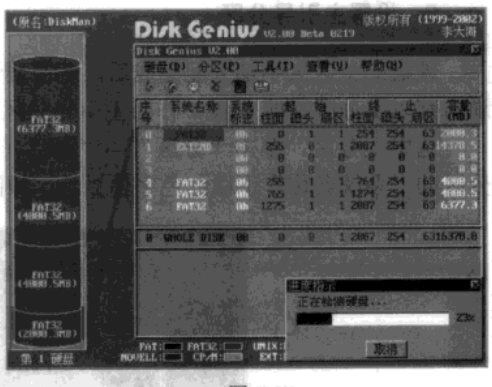


图 2-96

检测完成后，Disk Genius 自动对该分区的可用空间进行计算，如图 2-97 所示。计算完成后弹出“格式化完成”提示对话框，如图 2-98 所示。

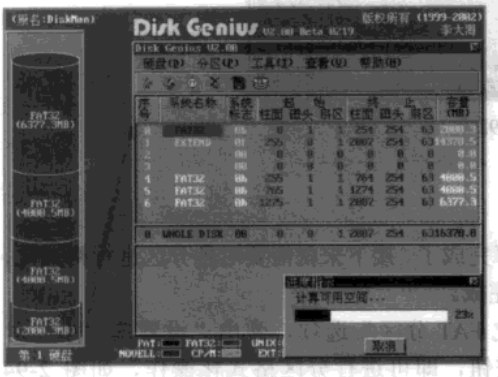


图 2-97

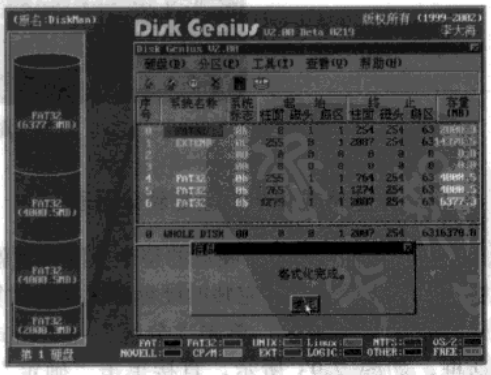


图 2-98

单击“确定”按钮，就完成了主分区的格式化。利用同样的方法对剩下的各逻辑分区进行逐一格式化。所有的分区格式化完成后，单击“硬盘”→“存盘”选项，弹出“更新硬盘

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

分区表？”提示对话框，如图 2-99 所示。单击“是”按钮，就可以对硬盘的整个分区信息进行保存了，也就是将分区信息写入分区表中。接着会再次弹出“0 柱面 1 磁头 1 扇区存在一个引导记录，是否删除？”提示对话框，如图 2-100 所示。单击“是”按钮后，开始更新分区表信息。



图 2-99

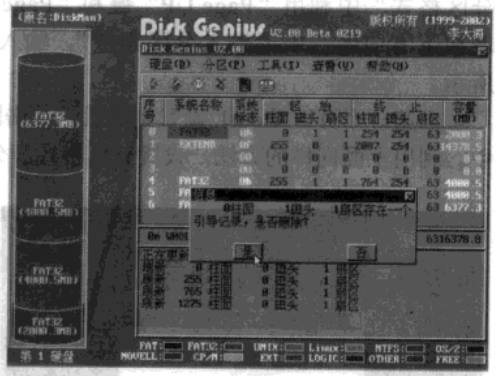


图 2-100

小知识 硬盘分区大小的分配操作，以及对分区表进行更新的操作只有在存盘后才会真正有效。如果不存盘，则可以任意对分区进行修改，不会对硬盘有任何影响。

对分区表进行更新后，单击“硬盘”→“退出”，重新启动计算机。在 DOS 提示符下利用 cd 和 dir 命令，就可以看到各分区的情况，接下来就可以安装 Windows 操作系统了。

案例 12 使用 F32 MAGIC 对 120GB 以上大硬盘进行快速分区

F32 MAGIC 是一款优秀的快速分区工具，用其对 120GB 以上容量的硬盘进行分区和格式化，只需要 30 多秒即可完成。

要使用 F32 MAGIC，先要将它拷入 DOS 启动盘中。接着通过 DOS 启动盘进入 DOS，运行 F32 MAGIC 就可以弹出 F32 MAGIC 的全中文界面，如图 2-101 所示。

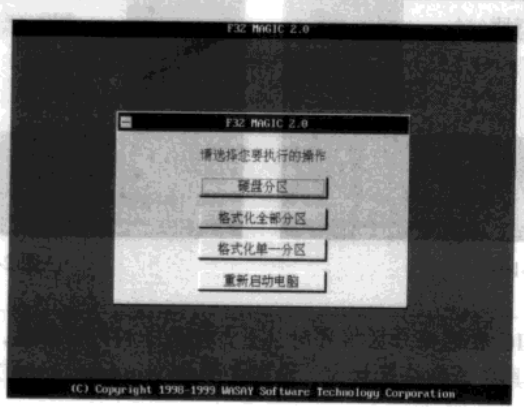


图 2-101

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1. 新建分区

要对硬盘进行分区，可在 F32 MAGIC 的全中文界面中，单击“硬盘分区”按钮进入“硬盘分区”窗口。在硬盘未分区之前，第一个分区标识为 Boot1。在下面的“选择分区格式”中利用“Page UP”键和“Page Down”键选择 FAT16、FAT32 分区格式，接着按下方向键选中“输入分区容量”，输入第一个分区的大小，如 2000MB，如图 2-102 所示。

当第一个分区 Boot1 设置完成后，单击回车键进入第二个分区（标识为 Boot2）的窗口中。利用上面同样的方法，设置分区格式和分区容量，如图 2-103 所示。

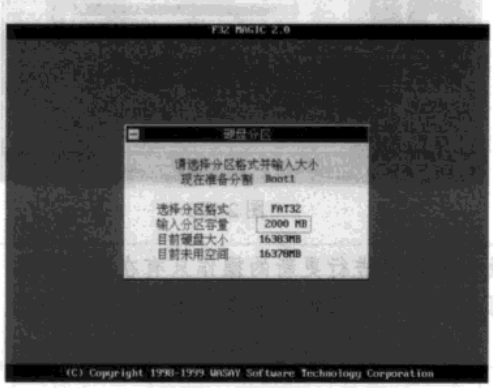


图 2-102

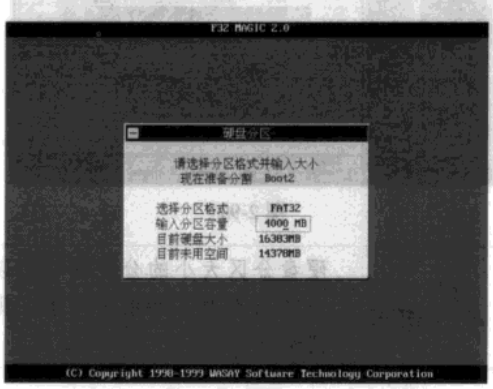


图 2-103

接下来根据弹出的设置窗口，再对其他分区进行分区格式、分区容量的设置，如图 2-104、图 2-105 所示，直到将整个硬盘分区完毕。



图 2-104

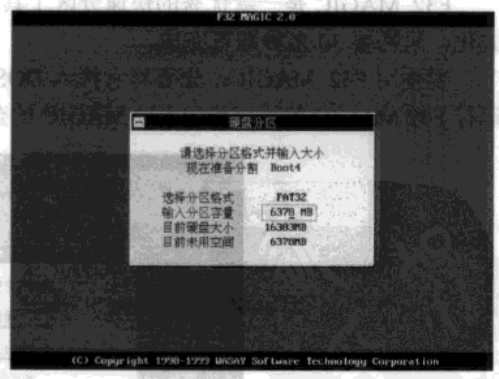


图 2-105

注意 F32 MAGIC 在选择分区格式时，不支持选择 NTFS 格式，只能在分区完成后利用其他工具来转换分区格式，或者在安装 Windows 2000/XP 时利用安装向导进行转换。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

当最后一个分区容量大小分配完成后，按回车键会弹出“硬盘准备分区，原有资料将丢失，要执行吗？”提示对话框，如图 2-106 所示。单击“是”按钮，即可按照硬盘容量的划分进行分区。若硬盘大小在 80GB 以下，执行分区根本不需要等待，立即会提示“分区执行完毕”，如图 2-107 所示。若大小为 120GB 以上，也只需要等待几秒钟即可。



图 2-106



图 2-107

2. 一次性格式化全部分区

硬盘分区完成后，可以利用 F32 MAGIC 提供的“格式化全部分区”和“格式化单一分区”功能来对分区进行格式化。按 Esc 键返回主菜单，选择“格式化全部分区”按钮，如图 2-108 所示。按回车键弹出“是否复制系统文件至硬盘中？”提示对话框，如图 2-109 所示。

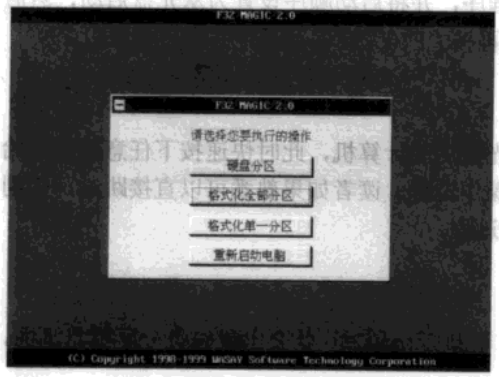


图 2-108



图 2-109

选择“是”，软件会提示“请在 A:中插入一张系统盘”，如图 2-110 所示。接着把准备好的一张系统盘放入 A:中，按回车键即可进行格式化，如图 2-111 所示。

整个分区和格式化过程才花了 15 秒钟（大小在 120GB 以上的硬盘也只需要 30 多秒钟）。接下来返回到主菜单界面，重新启动计算机，进入 DOS 提示符下，利用 cd、dir 命令查看各分区的情况。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 2-110

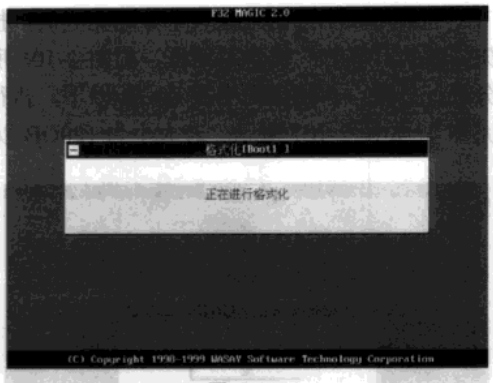


图 2-111

案例 13　使用 Windows 2000/XP/2003 安装盘对硬盘进行分区

大家都知道，一块新的硬盘必须经过分区和格式化才能安装操作系统、存储数据。因此，常常要使用诸如 Fdisk、PM 及 DM 等分区工具进行分区。然而，自从微软推出了 Windows 2000/XP/2003 之后，我们可以直接使用 Windows 2000/XP/2003 安装光盘，在安装 Windows 2000/XP/2003 系统时对硬盘进行分区和格式化。而且操作简单，全过程都是在简体中文平台上完成的，从而简化硬盘的前期处理过程。

这里，只重点介绍安装过程中的磁盘分区部分，Windows 2000/XP/2003 系统的详细安装过程，将在后面介绍。

1. 启动计算机，并在 CMOS 中设置光盘启动

开机后，按下“Del”键进入 CMOS 设置程序，并将启动顺序设置为从光盘启动，然后将 Windows 2000/XP/2003 安装光盘放入光驱，再按“F10”键保存设置并重启计算机。

2. 开始执行安装

重新启动计算机后，提示按下任意键将从光盘启动计算机，此时快速按下任意健即开始执行安装过程。从开始安装到磁盘分区之前的操作过程，读者如果熟悉可以直接跳过，否则请参照后面讲述的 Windows 2000/XP/2003 安装过程。

3. 执行磁盘分区

在安装过程中会提示接受协议，按下“F8”键接受协议后，就会出现磁盘分区信息画面，如图 2-112 所示。

在图 2-112 最底部，显示“未划分的空间”，即表明现在所使用的硬盘是未被分区的硬盘，此时就可根据提示进行分区及格式化。图中说明，在所显示的磁盘分区中可执行以下操作。

- 为系统选择安装分区。
- 按“C”键，建立磁盘分区。
- 按“D”键，删除选择的磁盘分区。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

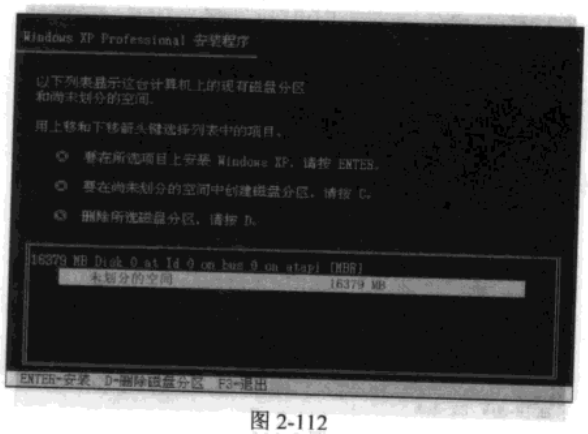


图 2-112

如果硬盘之前已做好分区，那么直接选择一个分区安装操作系统即可。但这里的硬盘之前没有分区，所以这时没有可用的分区供选择。这就要用到安装过程中的磁盘管理功能，也即利用安装光盘执行分区及格式化。

按下“C”键显示建立磁盘分区画面，如图 2-113 所示。根据提示，在创建磁盘分区大小处输入数值，单位是 MB。这一点和使用分区工具创建分区很相似，当输入完成后再按回车键，将显示分区信息，如图 2-114 所示。

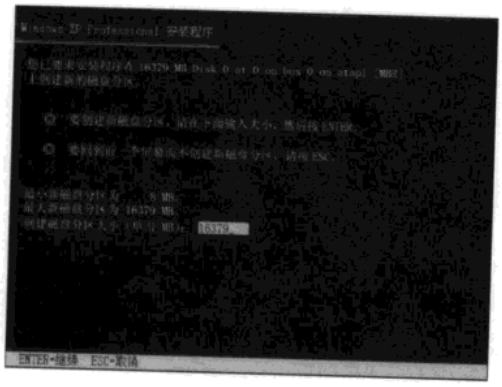


图 2-113

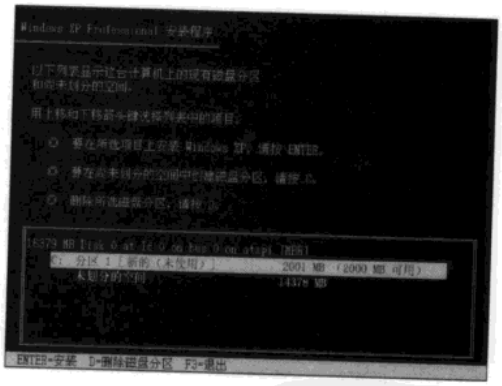


图 2-114

接下来可重复以上建立分区的步骤，直至将整个硬盘分区完成。

小知识

在使用 Windows 2000/XP/2003 安装光盘建立分区时，可以只建立一个用于安装操作系统的分区。其他未使用的空间，可在 Windows 操作系统安装以后，使用 Windows 2000/XP/2003 系统自带的“磁盘管理器”执行分区及格式化，而且速度很快。因此，为了提高效率，在此可以只建立一个系统分区，其他都不要建立。

当分区建立完成后，就要选择一个用于安装操作系统的分区，通常选 C，将光标移动到 C 分区后再按回车键，就可以看到提示格式化磁盘分区的画面，如图 2-115 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

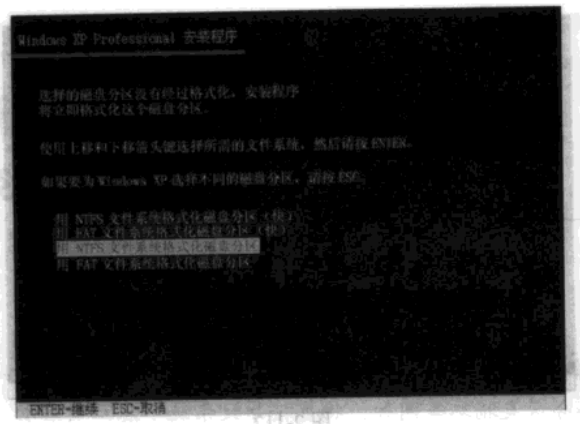
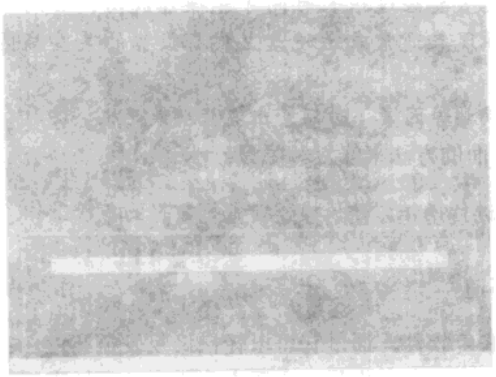
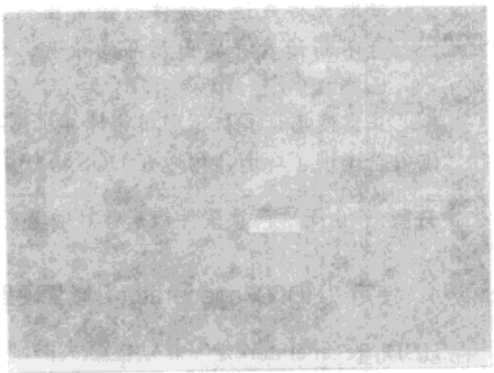


图 2-115

此时再根据提示选择合适的文件系统格式化磁盘分区，当格式化完成后即可继续安装，请参阅后面介绍的详细安装过程。

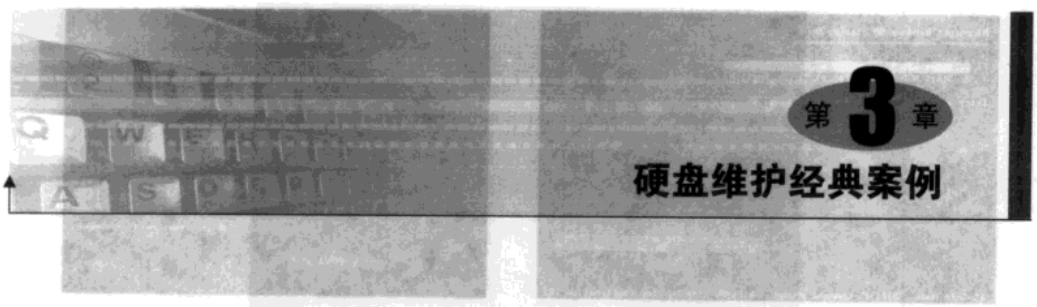
以上讲述的是如何在 Windows XP 安装过程中进行分区的建立、删除及格式化操作，Windows 2000/2003 系统的操作过程与之相同。希望读者能够掌握并灵活运用，以在安装系统时快人一步。





溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



第3章 硬盘维护经典案例

硬盘主要用来存储数据，也是操作系统能够得以运行的核心硬件之一。若硬盘出现物理坏道、主引导分区与分区表损坏等问题，将直接导致系统不能正确启动。而且一旦硬盘出现物理坏道而不能得到及时的修复，时间长了硬盘最终将被毁坏。所以，在硬盘出现问题时，及时进行维护和修复是非常重要的。

案例14 硬盘有坏道，系统不能引导、数据读取出错、系统频繁死机怎么办

硬盘经过长时间的使用，会出现物理扇区损坏（也就是通常称的“坏道”）。一旦硬盘物理扇区损坏，就会出现以下“症状”。

- 开机时系统不能通过硬盘启动，而用软盘启动后可以看到硬盘盘符，但无法进入。
- 读取文件或运行软件时经常出错，或者要经过很长时间才能操作成功，其间硬盘不断读盘并发出刺耳的杂音，这种现象通常表示硬盘上载有数据的某些扇区已损坏。
- 正常使用计算机（即排除计算机感染病毒等因素）时频繁出现蓝屏或死机。

硬盘若出现了坏道，可以在DOS下使用下面的方法来修复和隐藏。

注意 由于这两款软件都是针对磁盘底层进行操作，建议操作前做好数据的备份工作。

1. 使用“HDD Regenerator”修复硬盘坏道

HDD Regenerator是一款功能强大的硬盘修复软件，通过它可以轻松修复硬盘坏道。它采用了“反向磁化”工作原理，通过软件指令迫使磁头产生与磁介质本身相应的高低电平信号。通过多次的往复运动对损坏或者已失去磁性的硬盘扇区进行反复加磁，使得这些扇区的磁介质重新获得磁能力，从而达到让硬盘坏道工作能力再生的目的。

如果没有现成的HDD Regenerator启动盘，则可以事先制作一个。向软驱插入一张软盘，运行“HDD Regenerator”程序。接着从“Regenerator”菜单下进一步选择“Create Diskette”命令，并按照提示一步步操作，专用启动盘只需片刻即可制作完毕。

利用带HDD Regenerator的启动盘进入DOS，接着运行“HDD Regenerator”，进入图3-1所示的界面。直接按回车键，进入“硬盘坏道修复程序”，如图3-2所示。

按任意键后，进入图3-3所示的界面。在“请键入开始扫描位置的数值”处输入扫描的起始位置（这里是对已经知道坏道的具体位置而言的），这样可以节约扫描时间。软件的默认方式是从零磁道开始扫描。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

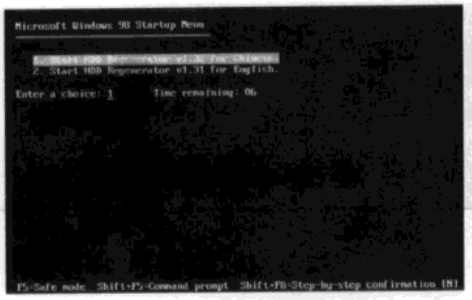


图 3-1



图 3-2

在扫描过程中可随时按下“Ctrl＋Break”组合键停止扫描，如图 3-4 所示。

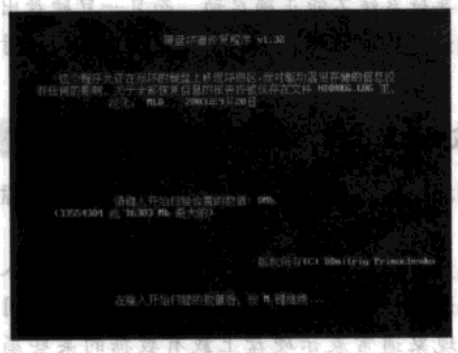


图 3-3

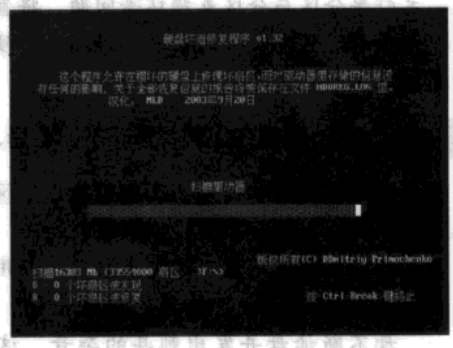


图 3-4

当 HDD Regenerator 软件扫描到硬盘坏道时会在进度条上显示红色的“B”字符，随后就开始自动修复，修复好以后会以蓝色的“R”字符标注。扫描并修复完以后就可以正常使用硬盘了。

2．使用“硬盘坏道修复器（HDDSPEED）”修复硬盘坏道

HDDSPEED 是一款比较专业的硬盘坏道修复工具，并且简单易用，红字表示发现的坏道，蓝字表示修好的坏道。

图 3-5 所示的是“HDDSPEED”主界面。直接按回车键，进入如图 3-6 所示的界面，再按回车键。

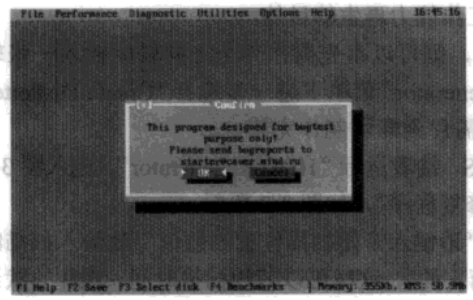


图 3-5

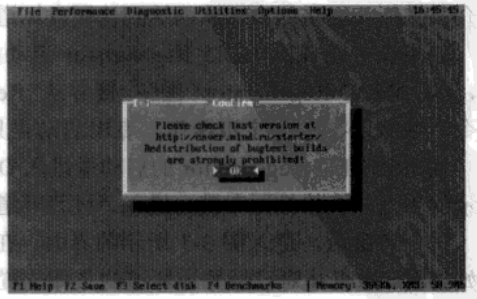


图 3-6

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如果对硬盘坏道进行修复，在图 3-7 所示的界面中中单击“Select”按钮，HDDSPEED 就开始对硬盘进行扫描，发现有坏道即可对坏道进行修复，修复后的坏道以蓝色表示，并弹出一个对话框，如图 3-8 所示。

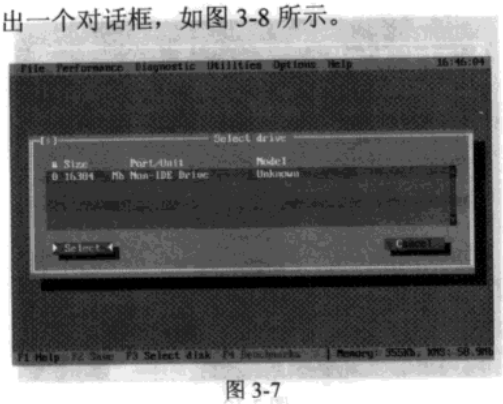


图 3-7

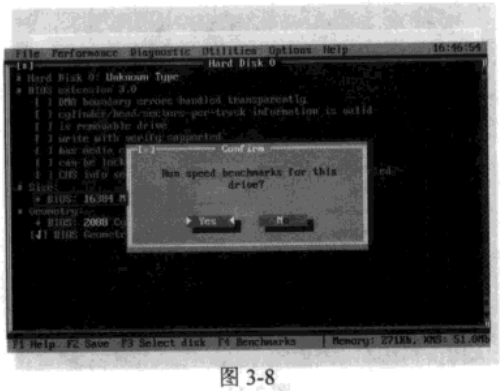


图 3-8

3. 使用 PM、Disk Genius 来隐藏硬盘坏道

若硬盘上出现了无法修复的坏簇或物理坏道，可用一些硬盘维护软件（如 PM、Disk Genius 等）将这些坏道单独分为一个区并隐藏起来，这样可延长硬盘使用寿命。这里以 PM 分区软件进行介绍。

进入 PM 主界面中，单击“Operations”→“Check for Errors”命令（如图 3-9 所示），算出坏簇在硬盘上的位置。

然后，单击“Operations”→“Advanced”→“Bad Sector Retest”命令（如图 3-10 所示），再次对坏道进行检测。

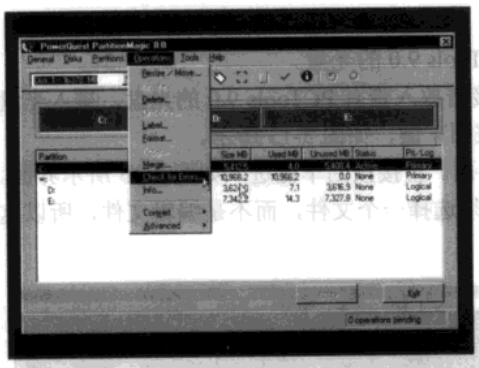


图 3-9

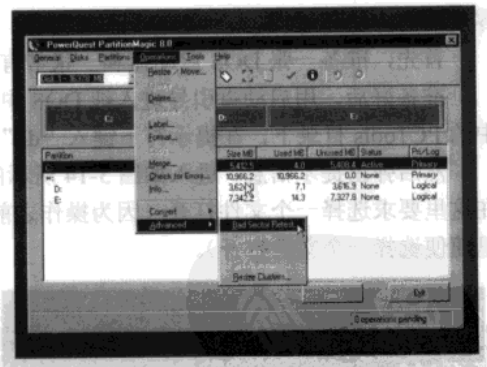


图 3-10

通过上面两步操作，就可以确定坏道所在的位置。然后选中坏道所在的盘符，单击“Operations”→“Resize/Move”命令（或工具栏中的按钮），打开“Resize/Move Partition”对话框，如图 3-11 所示。

通过对话框调整分区大小，把分区中所在的坏道划分出来，成为单独的一个分区。依此类推把其他分区中的坏道也划分出来。坏道划分出来成为一个单独分区后，再把这些坏道分区隐藏起来。具体操作是：选中单独的坏道分区，单击鼠标右键，在弹出的菜单中选中

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

“Advanced”子菜单下的“Hide Partition”命令，如图 3-12 所示。这样就能保证有严重坏道的硬盘正常使用，并避免因系统频繁地去读写坏道而扩展坏道的面积。

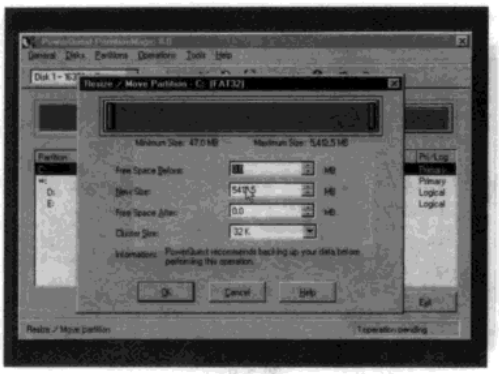


图 3-11

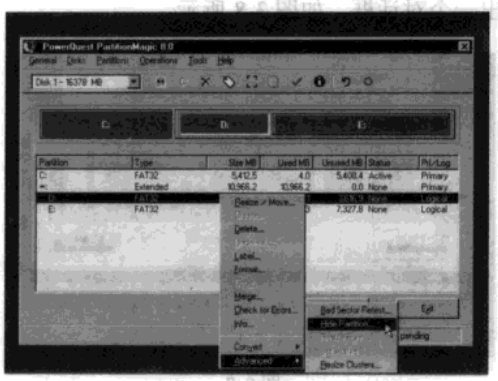


图 3-12

案例 15　硬盘零磁道损坏，无法引导怎么办

零磁道处于硬盘上一个非常重要的位置，硬盘的主引导记录（MBR）就在这个位置上。MBR 位于硬盘的 0 磁道 0 柱面 1 扇区，其中存放着硬盘主引导程序和硬盘分区表。在总共 512B 的硬盘主引导记录扇区中，446B 属于硬盘主引导程序，64B 属于硬盘分区表（DPT），2B（55AA）属于分区结束标志。由此可见，零磁道一旦受损，将使硬盘的主引导程序和分区表信息遭到严重破坏，从而导致硬盘无法引导。

在零磁道损坏的情况下，并不是没有办法进行修补。在 PCTools 里面有一个叫做 DE（DiskEdit）的工具，可以用来修复零磁道损坏的硬盘。下面带读者一起学习用 DiskEdit 修复零磁道的方法和过程。

首先，准备一张 DOS 启动盘和一张带有 PCTools 9.0 的光盘。

准备好后，用启动盘引导进入纯 DOS 中，接着放入带有 PCTools 9.0 的光盘，进入光盘中的 PCTools 目录下，在提示符下键入“de”，按回车键，如图 3-13 所示。

然后弹出提示信息，进入如图 3-14 所示的界面。直接按回车键进入如图 3-15 所示界面。在这里要求选择一个文件打开（因为操作之前必须选择一个文件，而不是编辑文件，所以这里随便选择一个文件打开）。

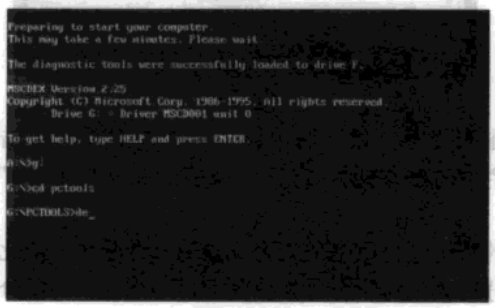


图 3-13

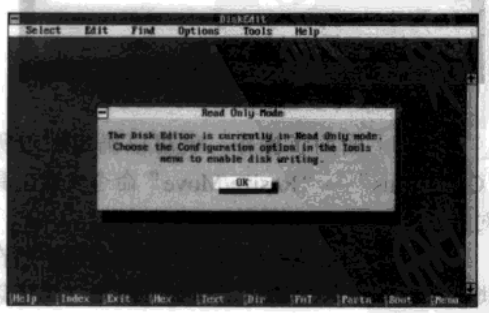


图 3-14

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

按键盘中的“Alt”键激活菜单，选择“Options”菜单下的“Configuration”（配置）选项，如图 3-16 所示。

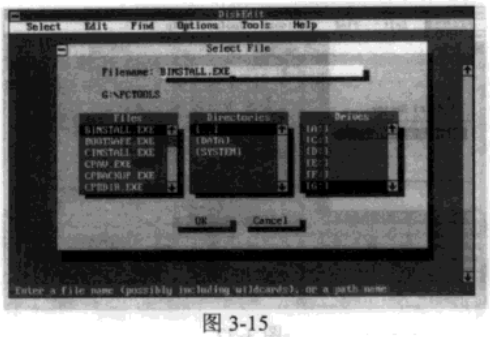


图 3-15

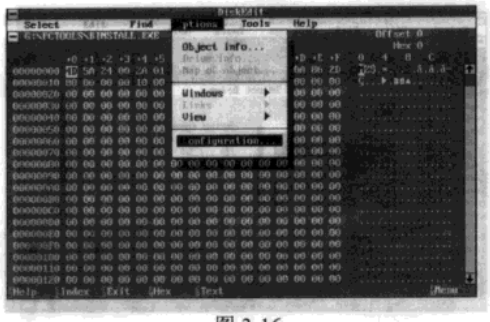


图 3-16

这时进入如图 3-17 所示的界面，通过按“Tab”键切换到“Read Only”复选框中，按空格键去掉“Read Only”复选框前的“√”，如图 3-18 所示。

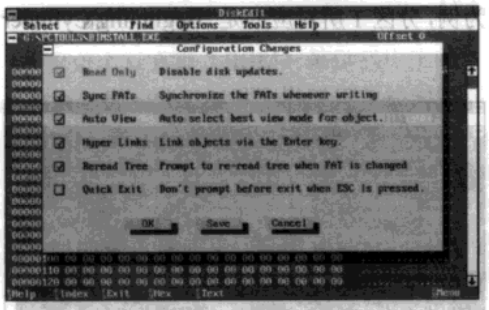


图 3-17

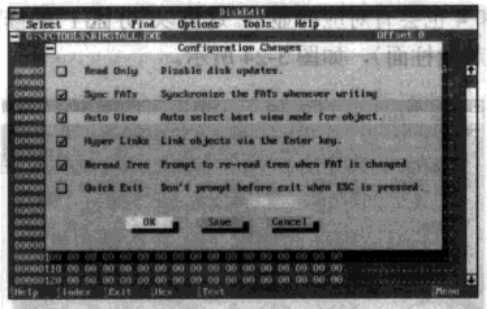


图 3-18

完成设置后，选择“OK”按钮，按回车键。再按“Alt”键激活菜单，选择“Select”菜单下的“Drive”选项，如图 3-19 所示，按回车键进入如图 3-20 所示的界面。

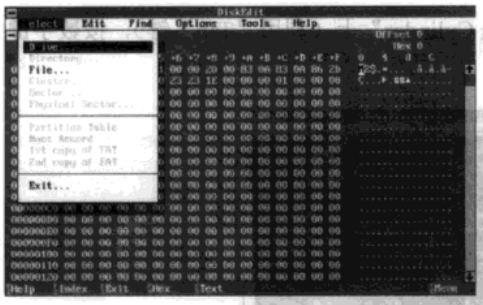


图 3-19

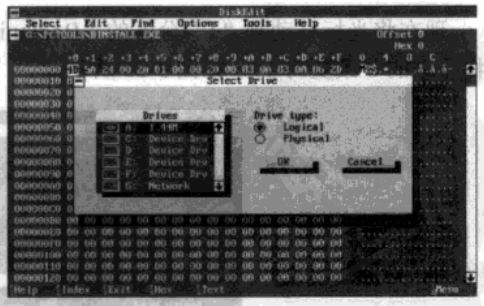


图 3-20

在图 3-20 中的“Drive type”选项下，利用“Tab”键将“Physical”复选框选中。接着再用“Tab”键切换到“Drives”选项下，并将下面的“Hard Disk”复选项选中，如图 3-21 所示。设置完成后，选择“OK”按钮，按回车键。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

再次使用键盘中的“Alt”键激活菜单，选择“Select”菜单下的“Partition Table”选项，如图 3-22 所示。

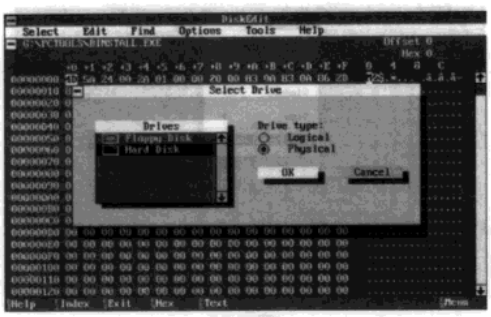


图 3-21

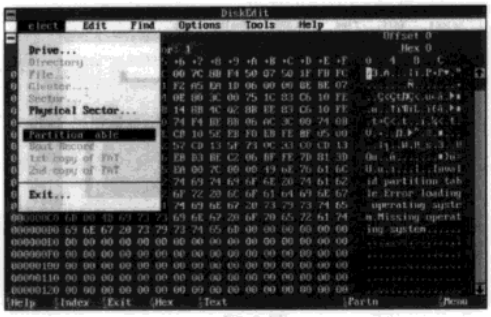


图 3-22

按回车键，进入如图 3-23 所示界面中，在此界面中可以看到分区表的相关信息。如果硬盘划分了主分区和扩展分区，那么分区 1 和 2 对应的都会有信息，如果有多个主分区，那么 3 和 4 也会有对应的显示。这里以“分区 1”的修复为例，分区 1 所对应的是“Beginning Cylinder”（起始柱面），如图 3-24 所示。

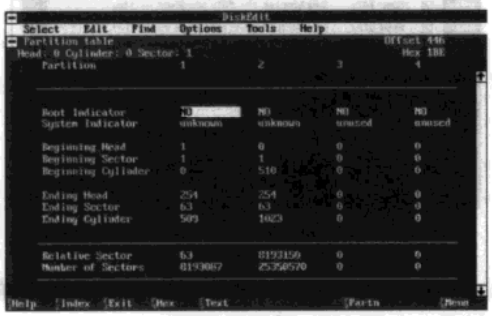


图 3-23

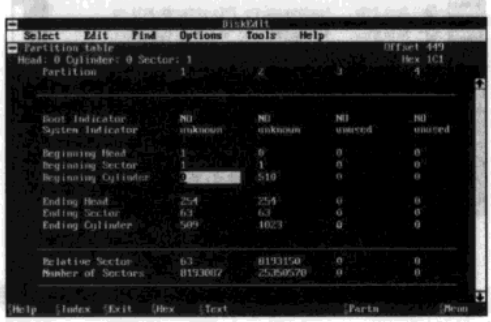


图 3-24

现在将光标移动到“1”分区的“Beginning Cylinder”上（利用“Tab”键），按数字键 1（将原来的 0 改变为 1），如图 3-25 所示。

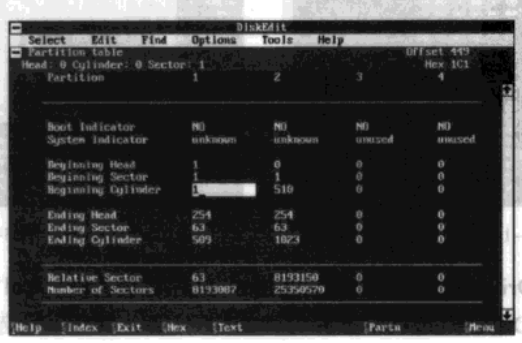


图 3-25

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

细心的朋友一定会发现，通过上面的操作只是改变了硬盘的起始柱面，DiskEdit 修复功能就是如此。理解了这点，当 1 磁道损坏时，那么可以在这里键入 2 或 3，其他同理。

修改之后按回车键，这时弹出提示信息，询问用户是否保存更改。选择“Save”按钮（如图 3-26 所示），按回车键确定即可。

按“Esc”键退出，系统会询问是否真的退出，如图 3-27 所示，选择“OK”按钮按回车键确定即可。



图 3-26



图 3-27

重新启动，按“Delete”键进入“CMOS”设置中，让“CMOS”重新自动检测一下硬盘设置，应该可以看到“Cylinder”（柱面）数量比原来减少了 1，保存设置并退出 CMOS。然后对硬盘重新分区，再格式化，修复操作就完成了。

注意 修复之后一定要在“CMOS”里面重新检测一次硬盘，再分区和格式化，因为只有对硬盘进行格式化后才能把分区表的信息写入 1 扇区。

案例 16 硬盘主引导扇区损坏，系统无法引导怎么办

当硬盘主引导扇区被损坏后，计算机启动时将无法正常地引导系统。若在硬盘损坏之前已经对主引导扇区作了备份，那么在损坏后可以对硬盘主引导扇区进行还原操作（如何备份、还原主引导扇区，可以参考第 6 章）；若没有备份，则可以通过下面的方法对主引导扇区进行修复或重建。

1. 修复主引导扇区

三茗硬盘医生是一款优秀的硬盘修复工具，不但可以对硬盘进行诊断分析，还可以修复主引导扇区、系统引导记录、分区表和文件分配表。

三茗硬盘医生只有 17KB 大小，可以从各大主流网站下载，如华军软件园、PCHome 等。下载后，复制到 DOS 启动盘中，利用启动盘进入 DOS 下，运行 hdd21.com 或 hdd21.exe，即可进入“三茗硬盘医生”主界面，如图 3-28 所示。在主界面中选择“修理硬盘”按钮，按回车键，进入“请选择需要修理的选项”窗口中，如图 3-29 所示。

若要修复主引导记录，按键盘空格键，将“主引导记录（位于 0 柱面 0 磁头 1 扇区）”左边的“不选”改为“选中”。若还要对系统引导记录、分区表、文件分配表进行修复，利用同样的方法将对应的“不选”改为“选中”，如图 3-30 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

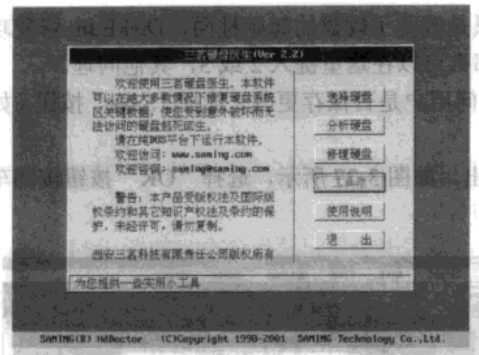


图 3-28

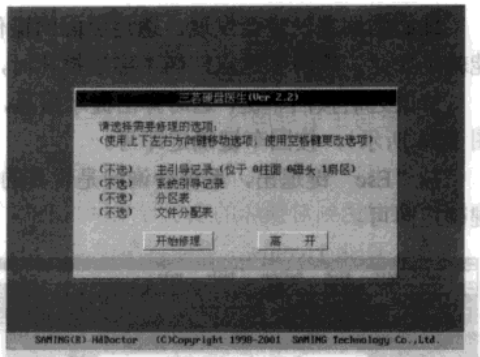


图 3-29

接着，选中“开始修理”按钮，按回车键，系统提示“请问是否需要在修理前对硬盘将修理部分进行备份？”，如图 3-31 所示。

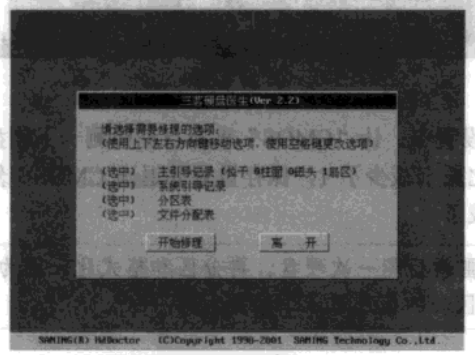


图 3-30



图 3-31

这里推荐“创建备份”，以免在修理过程中出现其他问题而导致不能正确修理。三茗硬盘医生会将备份的文件保存到软件默认的位置处，备份完毕后弹出提示信息，如图 3-32 所示。

选中“确定”按钮按回车键即可开始对硬盘的主引导扇区、系统引导记录等进行修理，修理结束后自动弹出提示信息，如图 3-33 所示。

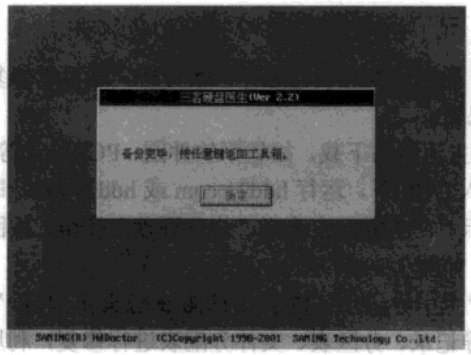


图 3-32

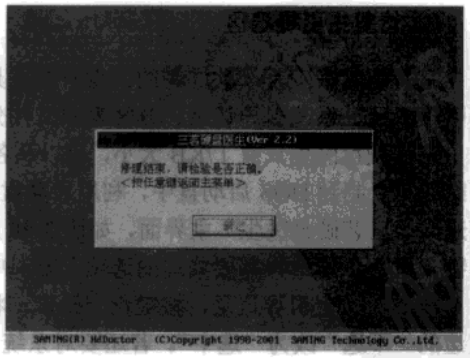


图 3-33

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

选中“确定”按钮按回车键完成对硬盘主引导扇区、系统引导记录等的修理。退出三茗硬盘医生，重新启动系统即可。

2. 重写主引导扇区

如果用户手中有 Disk Genius 工具，可以使用它的“重写主引导扇区”功能来重建主引导扇区，从而达到对损坏的主引导扇区进行修复的目的。

进入 Disk Genius 主界面，单击“工具”→“重写主引导记录”命令，如图 3-34 所示。接着弹出“重建硬盘主引导记录（MBR）？”提示对话框，如图 3-35 所示。

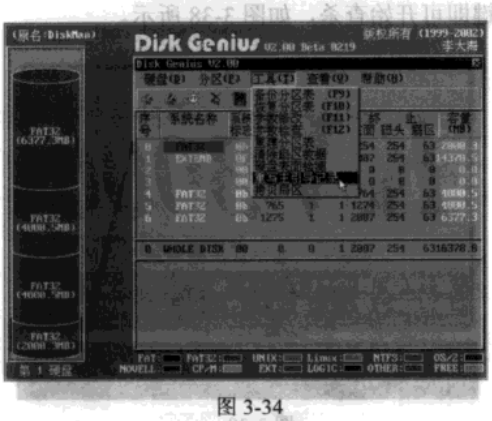


图 3-34



图 3-35

单击“确定”按钮，即可开始重写硬盘主引导扇区记录。重写完成后，在 Disk Genius 下可以看到“刷新 0 柱面 0 磁头 1 扇区”信息，如图 3-36 所示，说明硬盘主引导扇区已经修复完成，重新启动系统即可。

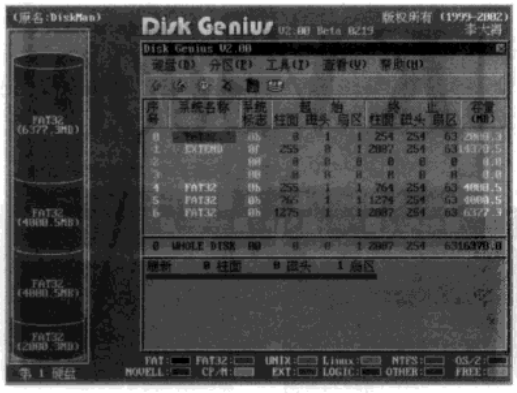


图 3-36

最后，单击“硬盘”→“存盘”命令即可。

案例 17 主引导扇区、分区表感染病毒，硬盘无法引导怎么办

当主引导扇区、分区表被病毒感染后，会导致硬盘主引导扇区和分区表被损坏，硬盘不

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

能引导。遇到这样的情况，可以先用 KV3000 对病毒进行查杀，然后再对主引导扇区、分区表进行修复。

1. 利用 KV3000 查杀病毒

将 KV3000 复制到 DOS 启动盘中。接着利用启动盘进入 DOS，运行 KV3000，进入 KV3000 的主界面，如图 3-37 所示。

KV3000 提供了 4 种查毒功能，分别是扩展查毒、快速查毒、杀毒、查（com、exe）毒。这里推荐使用“杀毒”功能来对硬盘进行查杀，先按键盘中的“F3”键，接着选择要查杀的分区，如对 C 分区进行查杀，按下键盘上的 C 键即可开始查杀，如图 3-38 所示。



图 3-37



图 3-38

在对 C 分区进行查杀时，如果有病毒，KV3000 会自动进行清除。当 C 分区查杀完成后，会在界面下方显示相关的信息，如图 3-39 所示。若有病毒被查杀或清除，会在“Kill or Clean”后显示查杀或消除的病毒个数。



图 3-39

利用同样的方法，再对其他分区逐一进行查杀。

2. 利用 KV3000 修复主引导扇区、分区表

主引导扇区、分区表的病毒被查杀后，就可以利用 KV3000 的修复功能修复主引导扇区、

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

分区表信息。

（1）利用 KV3000 修复硬盘主引导区

在 KV3000 主界面中，按键盘上的“F6”键，就可查看已经不能引导的硬盘隐含扇区，即查看硬盘 0 盘 0 柱 1 扇区的引导信息是否正常，如图 3-40 所示。主引导信息是硬盘引导系统的起点，比较重要的是两个标志，即 80H 和 55AA。



图 3-40

注意 在做这件事情之前，必须先用 KV3000/b 的格式将当前硬盘 0 面 0 柱 1 扇区的内容备份到另一张软盘上。若修复后未解决问题，可用 KV3000 hdpt.dat 的方式将软盘上的原备份再复制回硬盘，恢复硬盘的原来状态。

小知识 80H：一般在偏移 1BE 处，80 是分区激活的标志，表示系统可引导，且整个分区表只能有一个 80H 标记。

55AA：用来表示主引导信息是一个有效的记录。另外，各个分区自身的引导信息也是以 55AA 结束。

如果在硬盘的 0 面 0 柱 1 扇区没有找到图 3-40 中所示的第 2 和第 3 关键代码，说明 0 面 0 柱 1 扇区已经被病毒破坏。这时可以使用“PageDown”或“PageUp”两个翻页键，在硬盘的隐含扇区内查找，看能否找到被引导区病毒搬走的硬盘主引导信息。

小知识 一般情况下，硬盘的隐含扇区只有 0 面 0 柱 1 扇区有用，主要被用来做主引导扇区。0 面 0 柱 2 扇区以后的隐含扇区是空闲区，部分病毒主体有时隐藏在这些空闲区内。只要 0 面 0 柱 1 扇区中的病毒头被杀毒软件杀掉，就再也没有病毒头来调用，那么，2 扇区以后的这些病毒主体就成为无“头”的病毒“僵尸”，不具攻击性。

有时病毒会占用或加密了 0 面 0 柱 1 扇区，将原主引导信息搬到其后某一空闲的隐含扇区上。这时只要将主引导信息再搬回去，将病毒头覆盖掉，即可恢复主引导信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

上述所说的第 1 关键代码，可用 KV3000/k 指令来修复或生成。这里主要是查看有没有上述表中所说的第 2 和第 3 关键代码。如有，会在表中出现闪动的红色“80”和“55aa”，并响一声来给予提示，下行会出现“F9 = save to side 0 cylinder 0 sector 1 !!!”提示。这时，按一下“F9”键，就可将刚找到的原硬盘主引信息，覆盖到硬盘 0 面 0 柱 1 扇区中。然后，计算机会重新引导硬盘，恢复硬盘的启动性能（用启动盘引导后也能进入硬盘）。

在硬盘能正常启动时，应该备份硬盘主引导信息，以防不测。

命令格式为：KV3000/B；KV3000/HDPT.DAT

小知识

该命令将向 A 盘备份一个无病毒的硬盘主引导信息文件，名称分别为 HDPT.DAT 和 HFBOOT.DAT。当硬盘主引导信息被病毒破坏或主引导记录被损坏，导致硬盘不能启动时，使用“KV3000/A:\HDPT.DAT”命令格式恢复已经被破坏的硬盘，可解决大部分主引导信息被损坏、系统不能启动的问题。

有时硬盘能启动，KV3000 的智能扫描系统查出内存有病毒，如果再用软盘引导计算机，反而不能进入硬盘，这就表明硬盘分区表被病毒加密。可再次运行 KV3000，按下“F6”键查看硬盘 0 面 0 柱 1 扇区主引导区信息，如果看到的主引导信息与正常情况有很大差别，说明主引导信息已被病毒加密，备份出来也没有用。

这时应该再用硬盘自行引导，硬盘引导区的病毒被激活，并驻留到内存，在内存有病毒的情况下，再运行 KV3000 并按“F6”键查看主引导信息。如看到的是病毒已经将硬盘主引导信息解密且显示正常了，再按“S”键，将病毒自行解密的硬盘主引导信息备份到 A 盘。备份完后，再用干净的带有 KV3000 的 DOS 启动盘引导计算机，用 KV3000/hdpt.dat 的格式，即可将刚备份的正常的主引导信息恢复到硬盘。

然后，再用 KV3000/k 的格式将已感染到软盘的引导区病毒杀掉。重新启动计算机，一切将恢复正常。

小知识

如果先前没有备份过硬盘主引导信息，且硬盘主引导信息被病毒破坏，整个硬盘的数据无法读取，而用上述方法也找不到原分区表。这时，可以找一块相同型号的硬盘，按原硬盘分区格式对该硬盘进行分区。然后用 KV3000/b 格式将硬盘主引导信息备份到软盘上，再用 KV3000/hdpt.dat 的格式恢复到不能启动的硬盘上，即可使硬盘起死回生。

（2）利用 KV3000 修复硬盘分区表

如果先前用 KV3000/b 的命令在软盘上备份过主引导记录，这时就可用 KV3000/hdpt.dat 命令恢复硬盘主引导记录。如果先前没有备份过硬盘主引导信息，这时可以用 KV3000 快速重建硬盘分区表。

在 KV3000 主界面中，按下键盘上的“F10”键，就可对系统的有关参数和硬盘分区表进行快速测试。如果硬盘分区表不正常，KV3000 会先将坏分区表保存到软盘上，再自动重建硬盘分区表，使硬盘起死回生。这里来看看利用 KV3000 重建硬盘分区表的具体操作。

按下键盘上的“F10”键，即进入测试界面，KV3000 会首先测试并显示当前系统的部分信息，最后检测硬盘分区表。如果正常，则会显示如下信息。

“hard disk partition table - ok!”，表明硬盘分区表正常。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



“press any key to return ... ”，提示按任意键返回。

若出现“no hard disk partition table （no 80h)！use F6=view hdpt.”，则表明硬盘没有分区表或没有引导标志“80”，可用“F6”功能键查看硬盘分区表；若同时或单独出现“no "55aa"! in hard disk partition table. use F6=view hdpt.”，表明在硬盘分区表扇区上没有分区表有效标志“55aa”，可用“F6”键查看硬盘分区表。

接着提示“fix hard disk partition table or disk c boot sector （Y/N）?”，询问是否要修复硬盘分区表或 C 盘引导扇区（Y/N），按下“Y”键进行修复，按“N”键退出。



若硬盘能正常引导，也无病毒，请不要按“Y”键，以免将特殊的硬盘分区表修出问题。

为了安全，修复前会提示用户先备份、后修复。

当按下“Y”键，出现 “insert a formatted diskette in drive a, pressed "Y" to save "error" partition table into floppy, filename hdpt.vir, "n" to exit,' continue?（Y/N）”提示信息，意思是在 A 驱动器中插入一张已格式化的软盘，去掉写保护，按“Y”键将把硬盘的不正确的主引导信息先备份在软盘上，名为 hdpt.vir；接着再按下“Y”键，会将当前硬盘原分区表备份到软盘上保存。



·如果软盘上已有同名的文件，将拒绝进行，此时则需重新换一张软盘。

备份的目的是为了保证安全，若修复得不对，可用 KV3000/hdpt.vir 的格式恢复原样。备份完后会立刻修复好分区表，当出现“fixing...ok!”时，大功告成，按任意键计算机会自动引导，就可以进入硬盘了。

KV3000 在修复硬盘主引导扇区（硬盘 0 面 0 道 1 扇区）的内容时，KV3000 不会改动其他任何地方的内容，所以使用 KV3000 重建硬盘分区表是比较安全可靠的。



若是由于病毒引起的硬盘分区表错误，也可以在 DOS 下直接使用“Fdisk /mbr”命令来修复硬盘分区表。不过，“Fdisk /mbr”命令只是恢复主分区表，并不会对它重新构建，因此只适用于主引导区记录被引导区型病毒破坏，或者主引导记录代码丢失的情况。

案例 18　分区表被破坏，如何重建

分区表被破坏后，除了对其进行修复外，还可以重建分区表。要重建分区表，就需要利用 Disk Genius 工具。

进入 Disk Genius 主界面后，单击“工具”→“重建分区表”命令（如图 3-41 所示），弹出提示信息窗口，如图 3-42 所示。

单击“继续”按钮提示选择重建分区表的方式，如自动方式和交互方式，如图 3-43 所示。若选择“自动方式”，Disk Genius 会自动搜索分区；若选择“交互方式”，Disk Genius 每当发现一个分区，就给出提示信息，请求用户选择是否保留。对于重建分区表，推荐选择“自动方式”。接着 Disk Genius 自动搜索硬盘中所有分区的分区表信息，如图 3-44 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

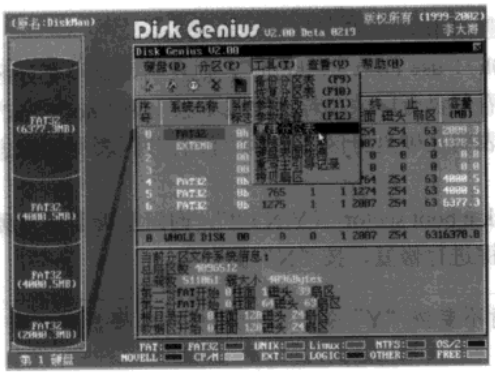


图 3-41

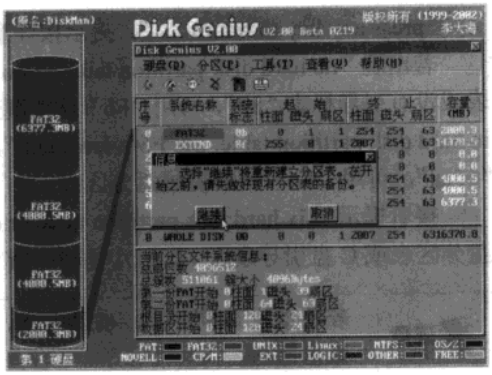


图 3-42

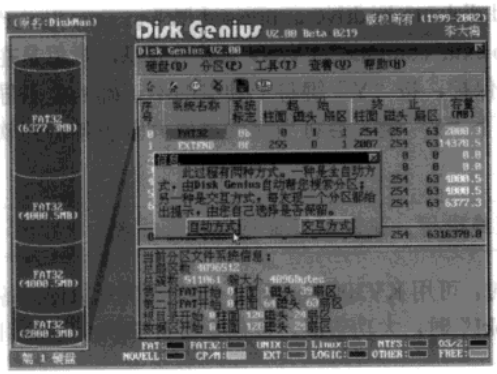


图 3-43

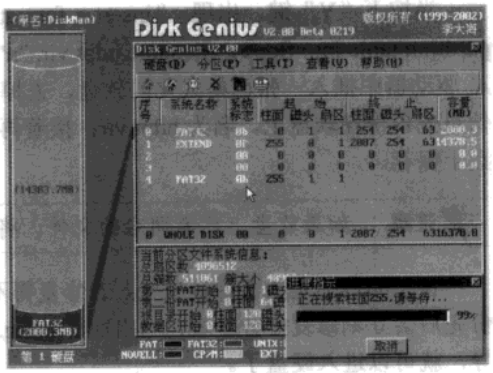


图 3-44

硬盘分区的分区表信息搜索完成后，Disk Genius 会自动进行重建。重建完成后，提示“分区表重建完毕，存盘后生效”，如图 3-45 所示。



图 3-45

最后，单击“硬盘”→“存盘”命令即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

案例19 为什么不能对硬盘进行重新分区操作

有些用户使用 fdisk 命令对硬盘进行重新分区时，却提示无法对硬盘进行重分区。选择 fdisk 下的“4. Display partition information”选项，只显示扩展分区，如图 3-46 所示。根据提示按下“Y”键后，却看不到扩展分区下的逻辑分区，如图 3-47 所示。

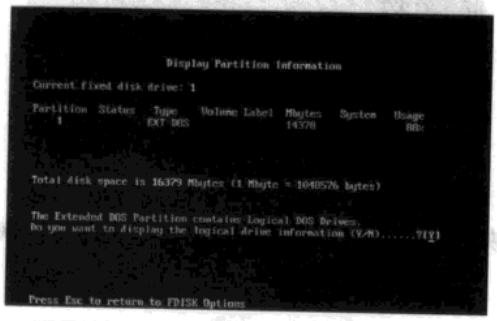


图 3-46

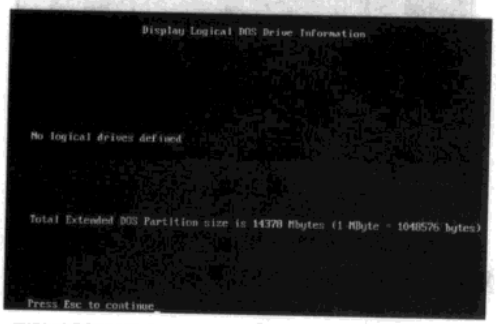


图 3-47

选择“3. Delete partition or Logical DOS Drive”→“2. Delete Extended DOS partition”选项，删除扩展分区，却提示“Cannot delete Extended DOS Partition while logical drives exist（当逻辑盘存在时不能删除扩展分区）”，如图 3-48 所示。

而接着再选择“3. Delete partition or Logical DOS Drive”→“3. Delete Logical DOS Drive（s）in the Extended Dos partition”选项，删除逻辑分区，却提示“No logical drives defined（没有定义的逻辑盘）”，如图 3-49 所示。

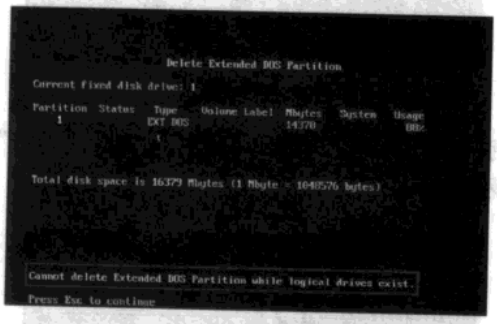


图 3-48

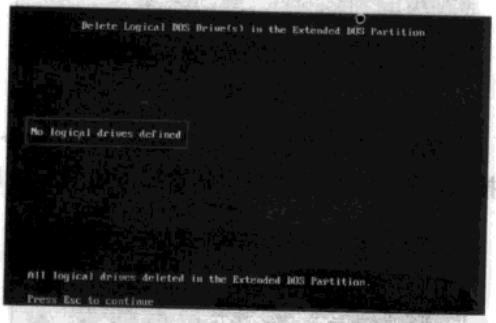


图 3-49

如果计算机出现这样的问题，说明在购买计算机时，装机人员专门分配了一定大小的分区作为系统的备份分区。当系统安装完成后，利用 Ghost 将系统备份到这个专门的分区中，然后利用 PQ 或 Disk Genius 隐藏了该分区。而 fdisk 本身是无法查看隐藏分区的，实际上该隐藏分区还在硬盘中没有删除，所以不能对硬盘重新分区。要想重新对硬盘进行分区，必须先将隐藏分区删除，具体的操作如下（这里以使用 Disk Genius 为例）。

进入 Disk Genius 后提示“请设定活动分区”，如图 3-50 所示，这是删除了主分区即活动分区所致。这里不用管，直接单击“确定”按钮，这时就可以看到硬盘中的一个隐藏分区，如图 3-51 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

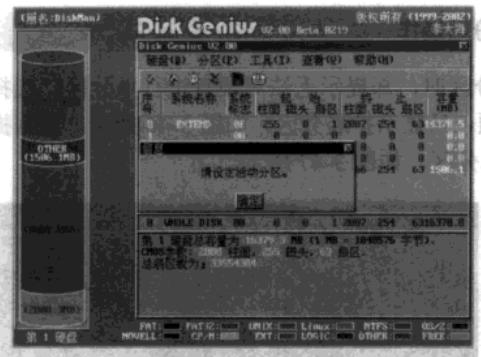


图 3-50



图 3-51

选中隐藏分区，单击“分区”→“隐藏（恢复）”命令，如图 3-52 所示。将隐藏分区恢复显示出来，如图 3-53 所示。

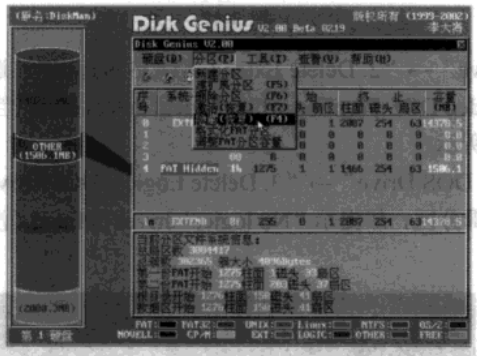


图 3-52



图 3-53

接着，单击“工具”→“删除分区”命令，弹出提示信息，如图 3-54 所示。单击“确定”按钮，将该分区从硬盘中删除掉，如图 3-55 所示。



图 3-54

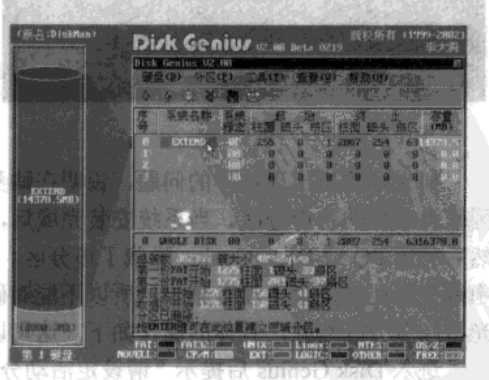


图 3-55

然后，选中扩展分区，单击“工具”→“删除分区”命令将扩展分区删除。这样硬盘中

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

所有的分区都已经被删除，如 3-56 所示。

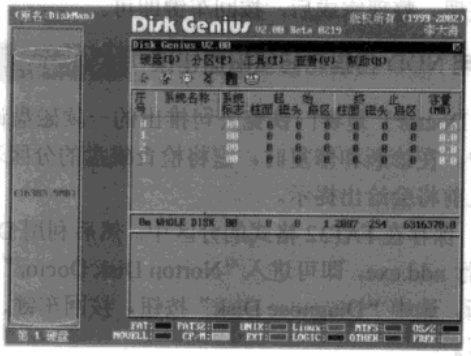


图 3-56

最后，用户可以利用 Disk Genius 对硬盘进行重新分区，也可以单击“硬盘”→“存盘”命令后，利用 fdisk 对硬盘进行重新分区即可。

案例 20 硬盘出现碎片，文件读取缓慢怎么办

硬盘在使用一段时间后，一般都会产生大量的碎片。而碎片并不是指磁盘出现了坏道，只是因拷贝、删除、移动文件等操作而产生的一些零碎文件，导致硬盘读写速度变慢。

当发现硬盘产生大量碎片时，一般都会使用 Windows 系统自带的“碎片整理”程序或其他碎片整理工具来进行整理。在 DOS 中，也有一个很不错的 defrag 命令，利用它可以在 DOS 下轻松地完成碎片整理工具，而且其整理速度比 Windows 系统中自带的碎片整理程序快得多。

注意 Defrag 是一个外部命令，必须先将其复制到 DOS 启动盘或硬盘中。利用 DOS 启动盘进入 DOS 运行此命令。

进入存放 defrag 命令的目录，在 DOS 提示符下输入 defrag 命令，即可打开图 3-57 所示的界面。

在图 3-57 所示的界面中，选择需要整理的盘符，然后选中“OK”按钮按回车键，对选中的盘符进行分析（流程方面和 Windows 自带的碎片整理工具差不多），如图 3-58 所示。

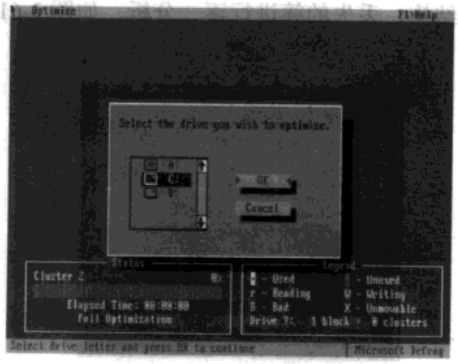


图 3-57

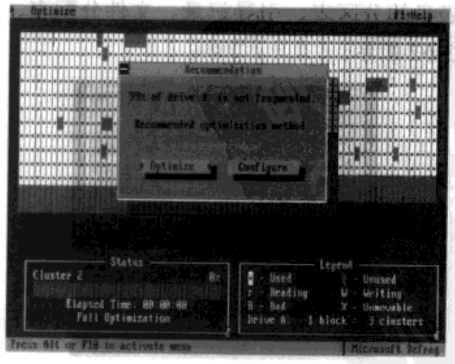


图 3-58

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

分析结束后，如果需要进行清理，再选择整理方式，接着选择“Begin Optimization”选项，开始进行硬盘碎片整理。整理完成后，按回车键即可。

案例 21　如何使用 NDD 扫描和修复磁盘错误

NDD（Norton Disk Doctor）是赛门铁克公司推出的一款磁盘诊断、修复工具，运行于 DOS 和 Windows 系统中。在诊断和修复时，它将检查磁盘的分区表和物理表面的每一处。检查到错误时，在修复之前将会给出提示。

先从网上下载 NDD，保存在 FAT32 格式的分区中。然后利用 DOS 启动盘进入 DOS，进入保存 NDD 的目录，运行 ndd.exe，即可进入“Norton Disk Doctor”主界面，如图 3-59 所示。

若要对硬盘进行诊断，选中“Diagnose Disk”按钮，按回车键，进入如图 3-60 所示的界面中，选择要诊断的分区。

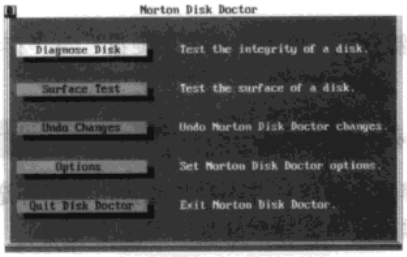


图 3-59

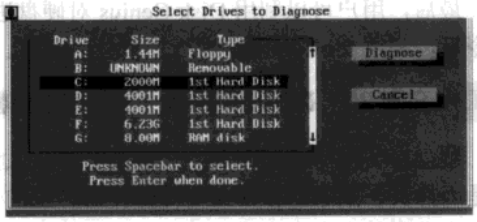


图 3-60

NDD 的主界面中的选项功能介绍如下。

Diagnose Disk：磁盘诊断，可以检测磁盘中所有的非物理性错误。

Surface Test：磁盘表面测试，对磁盘的物理表面进行扫描，以发现物理错误。

小知识

Undo Changes：取消改变，主要在使用 NDD 的过程中执行了不正确或不必要的操作时候使用。

Options：选项，在这里主要是对 NDD 进行设置。

Quit Disk Doctor：退出 NDD。

若先对 C 盘进行诊断，利用光标选中“C:”后，选中“Diagnose”按钮按回车键，即可对磁盘的分区表、引导记录、文件分配表、目录结构、丢失的簇进行逐一分析，如图 3-61、图 3-62 所示。

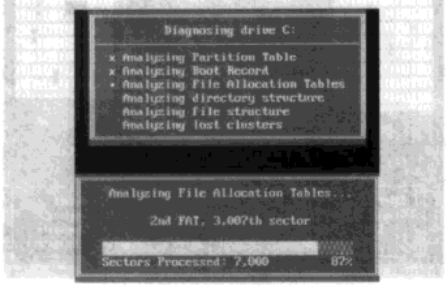


图 3-61

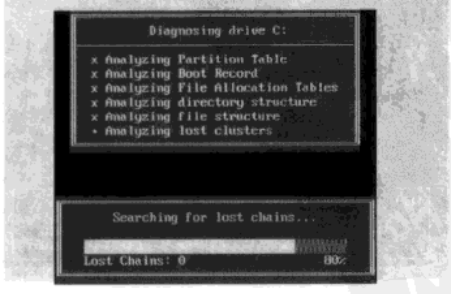


图 3-62

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在对磁盘分区表分析时，一旦检测到错误，NDD 会提示用户进行修复。一般来说，对于错误对象，NDD 会明确给出以下 3 个选项，分别是“Yes”（确定要修复）、“No”（跳过该错误并继续执行其后的诊断）、“Cancle”（放弃本次诊断任务）。

在选择“Yes”之后，NDD 会提示用户是否创建 Undo File（将本次修复经过保存为一个文件以便可以撤销修复）。若选择“OK”，表示创建，接着提示用户选择一个目录用以保存所生成的 Undo File 文件；若选择“Skip”，表示修复错误但放弃创建 Undo File 文件。

注意 当磁盘本身有潜在的物理错误时可能会导致创建 Undo File 失败。

当诊断任务完成后，NDD 会询问用户是否对磁盘表面扫描，如图 3-63 所示。若选择“Begin Test”，表示对磁盘进行扫描检测；若选择“Skip Test”，表示跳过此操作。

小知识 在使用“Diagnose Disk”对磁盘进行诊断后，一般所有的常规逻辑错误都会被发现并修复。若用户担心硬盘还存在潜在的物理错误或经常反复发生的错误，此时就有必要对磁盘表面进行检测了。

若继续对磁盘进行扫描检测，选中“Begin Test”按钮，按回车键，进入如图 3-64 所示的界面。



图 3-63

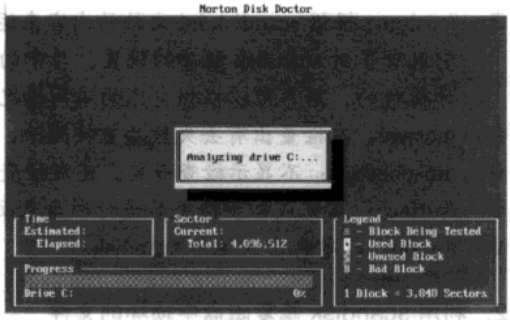


图 3-64

接下来开始对 C 盘进行全面的扫描检测，如图 3-65 所示。当发现错误时会弹出提示信息，提示用户是否进行修复。当对 C 盘扫描完成后，会给出如图 3-66 所示的信息，从而得知磁盘 C 分区哪里出现错误被修复（本例扫描检测结果为硬盘无错误）。

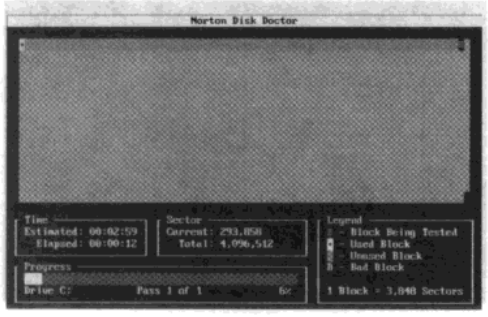


图 3-65

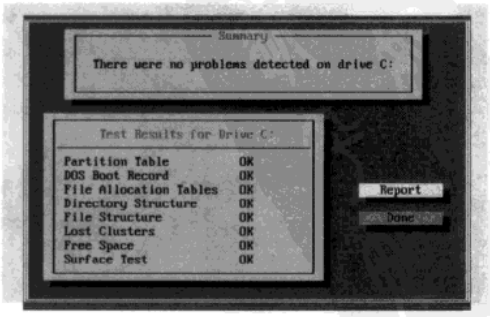


图 3-66

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

若用户要查看扫描检测后的报告，可以选择“Report”查看。如果用户还需要对其他盘符进行诊断和扫描检测，再次执行上面的操作过程即可。

案例 22　如何使用 scandisk 修复磁盘中损坏的文件

scandisk（scandisk.exe）是 DOS 下的外部命令，该命令用于对磁盘进行扫描和修复，能够解决大部分的磁盘文件损坏问题。如硬盘在使用过程中由于意外干扰或突然断电等原因，会产生一些文件链接错误，造成一些文件无法正常读取，此时就可以利用 scandisk 对磁盘进行扫描和修复。

1. 认识 scandisk 命令格式

命令格式：scandisk [盘符：] [参数]

参数说明如下。

- /fragment ［驱动器名:\路径\文件名］：使用这个参数可以显示文件是否包含有间断的块。
- /all：检查并修复所有的本地驱动器。
- /autofix：自动修复错误，即在修复时不会出现提示。
- /checkonly：仅仅检查磁盘，并不修复错误。
- /custom：根据 scandisk.ini 文件的内容来运行 scandisk。scandisk.ini 是一个文本文件，它包含了对 scandisk 程序的设置，其中的［custom］块是在加上“/custom”参数后才执行的，用户可以根据自己的不同情况来进行不同的设置。
- /nosave：在检查出有丢失簇后直接删除，并不转化为文件。
- /nosummary：不显示检查概要，完成检查后将直接退出程序。
- /surface：在完成初步检查后进行磁盘表面扫描。
- /mono：以单色形式运行 scandisk。

2. 利用 scandisk 修复磁盘中损坏的文件

将 scandisk 复制到启动盘中，利用 DOS 启动盘进入 DOS，在提示符下输入“scandisk /all /autofix /nosave /surface”，如图 3-67 所示。按回车键进入“Microsoft ScanDisk”界面，并开始对 C 分区的文件分配表、目录结构等进行检查，如图 3-68 所示。

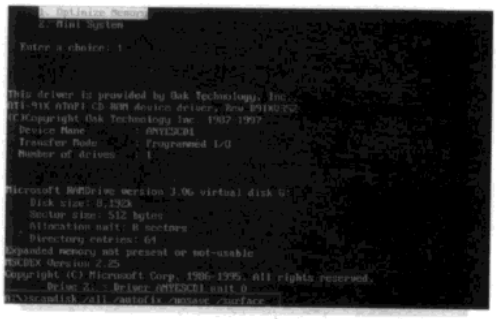


图 3-67



图 3-68

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

小知识 scandisk /all /autofix /nosave /surface 是指对磁盘进行全面检测，并自动修复，而且在检测时查出有丢失的簇时，直接进行删除。检测、修复完成后，对磁盘表面进行扫描。

检查过后，进入如图 3-69 所示界面中，scandisk 开始对 C 分区进行扫描检测和自动修复。当对 C 分区扫描检测、修复完成后，提示用户是否继续对磁盘其他分区进行扫描检测和自动修复，如图 3-70 所示。

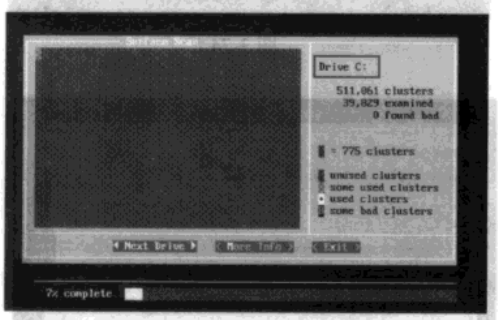


图 3-69

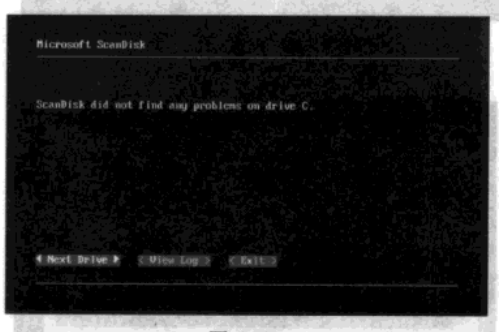


图 3-70

选中“Next Drive”按钮后按回车键，继续对 D 分区的文件分配表、目录结构等进行检查，如图 3-71 所示。检查过后，开始对 D 分区进行扫描检测和自动修复，如图 3-72 所示。



图 3-71

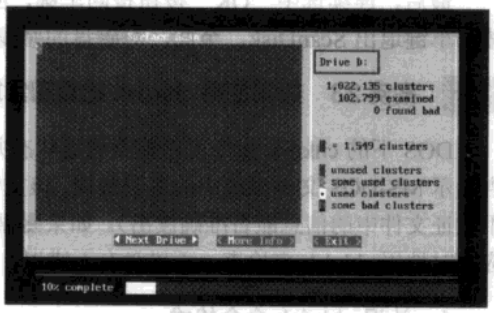


图 3-72

当对 D 分区扫描检测、修复完成后，同样提示用户是否继续对磁盘其他分区进行扫描检测和修复。选中“Next Drive”按钮按回车键后，继续对其他磁盘分区逐一进行扫描和修复，直到所有分区都扫描检测和修复完成。

在对最后一个分区进行扫描检测和自动修复后，用户可以选中“View Log”（查看日志）按钮，如图 3-73 所示。按回车键后，即可看到对磁盘进行扫描检测和修复的信息，如图 3-74 所示。

若用户想保存该日志，可以选中“Save Log”按钮，按回车键进入如图 3-75 所示的界面，然后直接按回车键，则默认将日志保存到 C:\SCANDISK.LOG，并弹出询问信息，如图 3-76 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

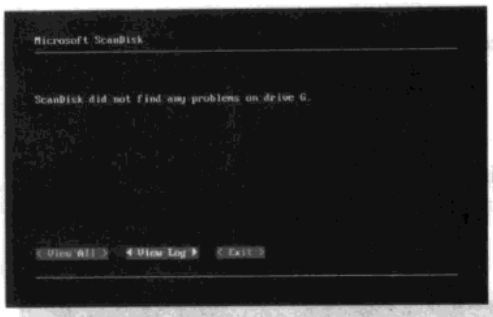


图 3-73

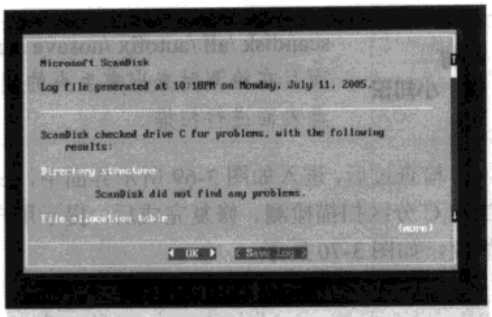


图 3-74

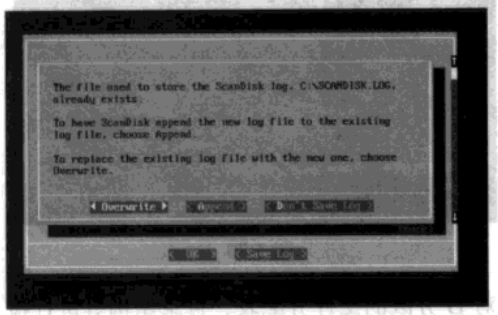


图 3-75

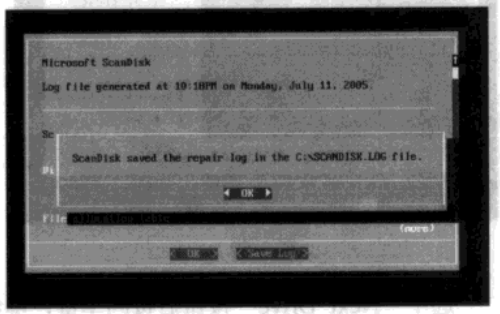


图 3-76

最后，连续选中“OK”按钮按回车键，回到如图 3-73 所示的界面。选中“Exit”按钮，按回车键退出 ScanDisk。至此，对磁盘的修复全部结束。

案例 23　如何使用 chkdsk 检查和修复磁盘错误

DOS 下的 chkdsk 命令可以检查磁盘状态并显示状态报告，还可以修复磁盘错误。状态报告显示 MS-DOS 文件系统中的逻辑错误，该文件系统由文件分配表（FAT）和目录组成（chkdsk 不验证文件中的信息能否准确读出）。如果磁盘有错误，chkdsk 便会给出一条警告信息。所以，应不时地用 chkdsk 来检查一下磁盘有无错误，以保证系统的正常运行。

1. 认识 chkdsk 命令格式

```
命令格式：chkdsk [盘符：] [参数]
```

参数说明如下。

- /f：修正磁盘错误。
- /v：检查磁盘时，显示每个目录下的文件。

2. 使用 chkdsk 检查和修复磁盘错误

利用 DOS 启动盘进入 DOS，若要检查磁盘某分区（如 C 分区）的信息，可以在提示符下输入“chkdsk c:”按回车键，即可显示 C 分区相关的信息，如图 3-77 所示。当遇到错误时，chkdsk 会暂停并显示提示信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

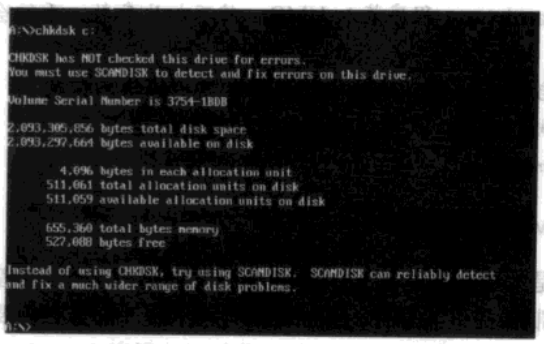


图 3-77

若要对某磁盘分区进行错误修复（如 C 分区），可以在提示符下输入 chkdsk c: /F<回车>，即可对 C 分区进行检查，并在遇到错误时进行修复。

小知识

chkdsk 命令只能找到文件系统中的逻辑错误，而不能查找磁盘物理错误。要查找磁盘物理错误，请使用 scandisk 程序。如果有两个文件或目录共用同一磁盘空间的记录，chkdsk 会报告有交叉链接文件。如果 chkdsk 发现有交叉链接文件存在，会提示“is cross linked on allocation unit”信息。chkdsk 不会修补交叉链接文件，即使是在指定了/F 参数的情况下。要修复交叉链接文件，需要运行 scandisk 程序，或者进行手动修复，然后复制文件到指定的文件夹中并删除原文件。

案例 24 如何使用 Smartdrv 设置磁盘缓存加速

Smartdrv.exe 是一个程序文件，用来在扩充内存中创建一个磁盘高速缓存区域，从而缩短读写硬盘的时间。Smartdrv.exe 可以通过命令行方式执行，还能完成通过 Config.sys 创建双缓冲。

1. 认识 Smartdrv 命令格式

```
Smartdrv [/E:区块大小][/B:BUFFER 大小] [/C] [/R] [/L] [/Q] [/V] [/S]
[init cache size] [win cache size] [Drive +/-]
```

- DRIVE +/- ：指定某一个磁盘拥有磁盘缓存功能，如果不加 +/- 就表示只允许读取缓存。
- /E：区块大小，指定 Smartdrv 在内存与磁盘之间移动数据时的每次基本搬移量。区块大小只能是 1024/2048/4096/8192 INIT CACHE SIZE ，启动 Smartdrv 时拥有磁盘高速缓冲区的大小单位是 KB。这个数值越大，磁盘存取工作的效果越好。
- /B：BUFFER SIZE，表示缓冲区的大小。缓冲区越大，占用常规内存越多，缺省是 16。
- /C：把内存中的所有缓冲区信息写入硬盘。
- /R：清除所有高速缓冲区内容，重新启动 Smartdrv。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- /L：不把 Smartdrv.exe 程序装入 UMB。若不加此参数，系统会自动把 Smartdrv.exe 调入 UMB；
- /V：设定在启动 Smartdrv 的时候，屏幕上显示的状态信息。
- /Q：不显示状态信息，只是当程序执行出错时才会显示。
- /S：显示附加信息。

2. 利用 Smartdrv 建立双重缓冲区

双重缓冲的作用是为那些不能在 EMM386 提供的内存中工作，或者以 386 增强模式运行的 Windows 的硬盘控制器提供兼容性。Smartdrv 的双重缓冲部分必须要装到常规内存中，占用 2KB 空间。在 Config.sys 中使用 Device 调入设备驱动程序 Smartdrv.exe 即可。

注意

用户不可以用 Devicehigh 装入，而应该用以下方法加装。

格式为：DEVICE=SMARTDRV.EXE /DOUBLE_BUFFER /D+

如果加载成功应该执行 Smartdrv.exe 程序，此时“Buffering”一栏会全部显示为“yes”。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第4章 Windows 系统维护经典案例

Windows 系统赋予了计算机硬件系统“灵魂”，从而使计算机得以广泛地应用。而这个“灵魂”一旦受到“伤害”，将直接导致整个计算机硬件系统不能正常运行，甚至会带来毁灭性的灾难，所以经常维护 Windows 系统是十分必要，也是必须的。

案例 25　在 DOS 下安装 Windows 2000/XP/2003 系统，直接运行 setup.exe 怎么不行

如果在计算机上只安装了一种操作系统，在系统被损坏后，一般都是在 DOS 下运行硬盘中的 Windows 2000/XP/2003 安装文件，或使用 Windows 2000/XP/2003 安装盘来安装系统。但是运行安装目录下的 setup.exe 时，却无法进行安装，这是因为安装文件坏了吗？其实不然，在 DOS 下安装 Windows 2000/XP/2003 时，不能像安装 Windows 98 一样直接运行 setup.exe 即可进入安装界面，而是需要先加载 Smartdrv.exe，然后运行 I386 目录下的 winnt.exe，才可进行安装（本案例以在 DOS 下从安装光盘中安装 Windows XP 系统为例）。

小知识　在进入 I386 目录之前，运行 smartdrv.exe 命令，可以加快 Windows 2000/XP/2003 的安装速度。smartdrv.exe 一般在 windows 98 的安装光盘中或是在 Windows 98 系统的“Windows”目录下。

利用 Windows 98 或启动盘启动计算机到 DOS 环境下，首先加载 Smartdrv.exe。在提示符下输入“smartdrv.exe”按回车键，如图 4-1 所示。

接着利用 DOS 命令下的 cd 命令，进入 Windows XP 安装目录下的 I386 文件夹中，运行 winnt.exe，如图 4-2 所示。



图 4-1

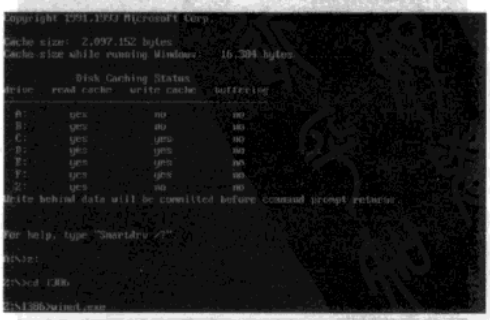


图 4-2

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

运行 winnt.exe 后，系统将会询问安装文件的来源，如图 4-3 所示。系统安装时，必须知道 Windows XP 安装文件的来源以便复制安装文件。缺省情况下，文件来源可以被自动检测到。

确认安装文件来源后，按回车键，这时系统开始复制安装文件到硬盘。复制文件需要一段时间，这时需要耐心等待。图 4-4 所示的界面提示文件复制的进度和当前正在复制的文件。

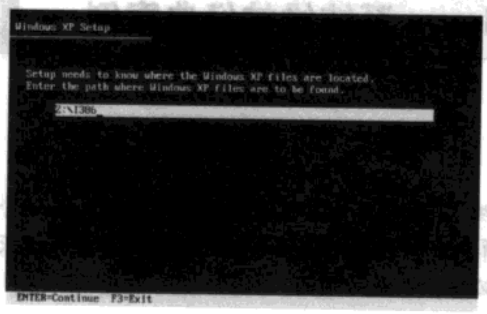


图 4-3

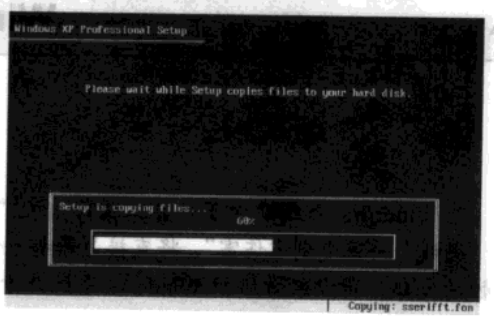


图 4-4

文件复制完成后，进入图 4-5 所示的界面，提示用户是否继续进行以下操作。按回车键后，重新启动计算机，接着进入图 4-6 所示的界面自动进行初始化配置。

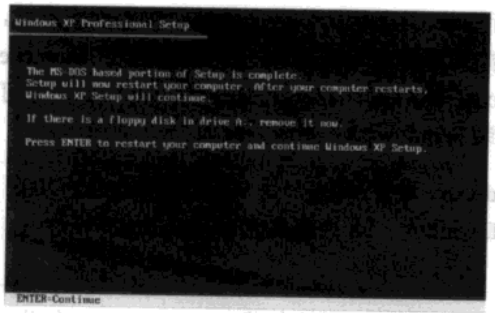


图 4-5

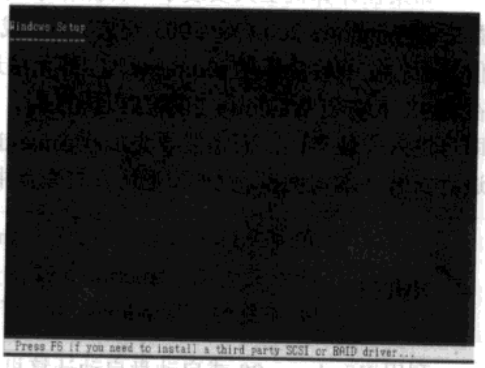


图 4-6

配置完成后，进入 Windows XP 安装向导，如图 4-7 所示。若安装 Windows XP，按回车键，这时开始检查磁盘配置，如图 4-8 所示。

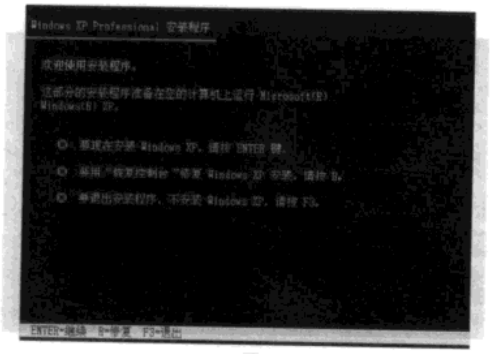


图 4-7

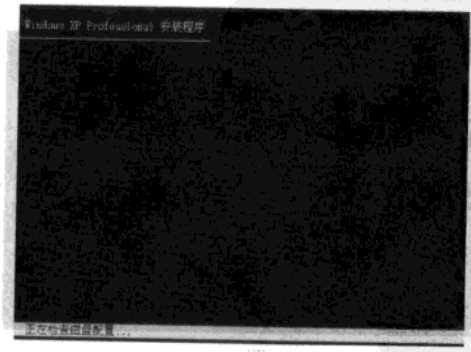


图 4-8

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

磁盘配置检查完毕后，接下来提示是否接受产品许可协议，如图 4-9 所示。按“F8”功能键接受该协议。接下来选择安装 Windows XP 的分区，如图 4-10 所示。

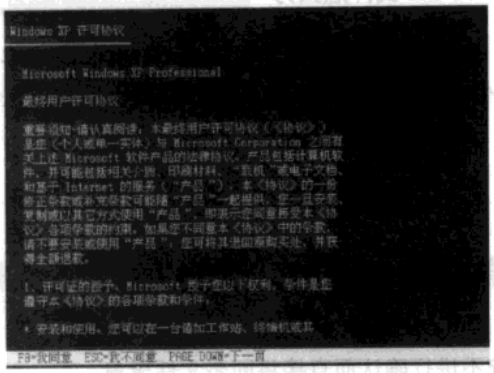


图 4-9

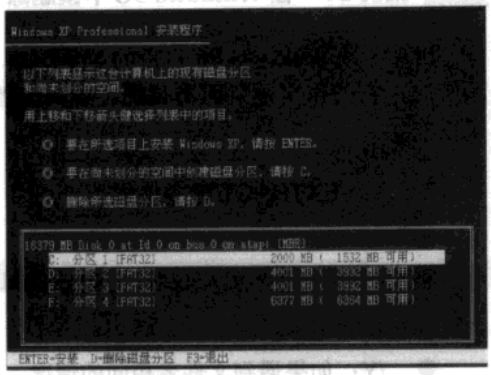


图 4-10

选择好安装 Windows XP 的分区后，按回车键，安装程序询问是否改变原有磁盘分区的文件系统。接下来的安装和配置步骤与从 Windows 98 中升级或安装 Windows XP 一样，都是向导化操作，至此就解决了不能在 DOS 直接运行 setup.exe 安装 Windows 2000/XP/2003 的问题。

案例 26 忘了 BIOS 密码怎么办

为了防止别人改动自己的计算机设置，一些读者为进入 BIOS 设置了密码。如果忘记了密码怎么办呢？也许有的用户会使用万能密码、放电、密码破解工具等方法来破解，其实可以在 DOS 下使用 debug 命令来解决这个问题。

利用 DOS 启动盘进入 DOS，进入 C 盘根目录，在提示符后依次输入图 4-11 所示的指令，每输入一行命令按一次回车键。



图 4-11

命令解析

```
debug          ；启动 debug 命令
-o 70 88       ；将错误的 88 数据写入到 70 端口中
-o 71 88       ；将错误的 88 数据写入到 71 端口中
-q             ；保存退出 debug
```

注意 70 和 71 是 CMOS 的两个端口，利用“o”语句将错误的数据（如 10、11、16、17、20 等）覆盖原有 CMOS 数据，致使 CMOS 读取数据出错而自动重置成没设密码的初始状态，从而达到破解目的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

退出 debug 命令后，重新启动计算机即可。

案例 27　在 Windows 98 下误删除了 pdos.def 文件怎么办

PDOS 是 Windows 98 自带的 MS-DOS 7.0 中的汉字系统，当手中没有 UCDOS 等汉字系统时，它的作用是显而易见的。如果读者不小心误删除了此文件，可以通过下面的方法来恢复。

1. 认识 EXTRACT 命令格式

```
命令格式：EXTRACT[/Y][/A][/D] [/E][/C]源文件名[目标文件][/L]目标路径
```

参数说明如下。

- /Y：如果遇到文件名相同的情况，系统不进行确认而直接将同名文件覆盖。
- /A：对源文件之后要提取的文件进行操作。
- /D：显示源文件中的具体内容。
- /E：单独展开指定的文件。
- /L：指定展开后的文件路径。
- /C：复制源文件到指定地点。
- 源文件名：源文件名指的是安装盘中后缀为.CAB 的压缩文件。
- 目标文件：目标文件指的是放在源文件中的被压缩文件。

2. 利用 EXTRACT 来提取压缩包中的 PDOS.DEF 文件

pdos.def 文件在 Windows 98 安装文件下的 win98_27.cab 压缩包中，需要通过 EXTRACT 命令来提取，并保存到“C:\”下。

首先，利用 DOS 启动盘进入 DOS，将 Windows 98 的安装光盘放入光驱，若硬盘中有 Windows 98 文件，则需确认其具体的路径。接着在提示符后输入“extract /e z:\os\win98\win98_27 .cab pdos.def /l c:\”，按回车键，开始从 win98_27.cab 压缩包中提取 pdos.def 文件，如图 4-12 所示。提取完成后保存到 C:\下。

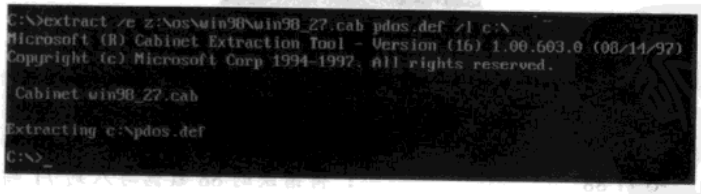


图 4-12

这里，“z:\os\win98\”是存放 win98_27.cab 文件的路程。

然后，在 DOS 下运行 edit 命令，进入文本编辑器中，打开 pdos.def 文件，将“c:\pdos”改写为“c:\windows\command”，如图 4-13 所示，存盘退出 edit 窗口。

最后，重新启动计算机即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

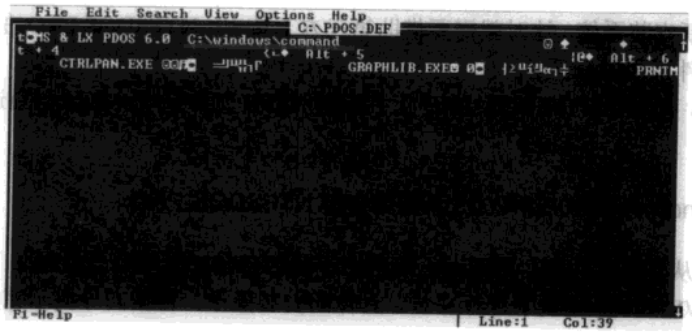


图 4-13

案例 28 系统文件被病毒感染后，在 Windows XP 下无法删除怎么办

目前很多计算机用户都使用 Windows XP 系统。虽然 Windows XP 的安全性相对较高，但是病毒还是无孔不入。系统遭受到病毒的攻击后，一般是感染系统文件，或者是在 System32 目录中自动生成带病毒的 DLL 文件。在 Windows XP 中是不能直接删除这些文件的（在 Windows 2000/2003 中也同样不能删除）。这时，可以进入纯 DOS 下（注意：这里不是指在 Windows XP 的命令提示符状态下）进行删除。具体的操作步骤如下。

首先，记住受病毒感染的系统文件，或自动生成的病毒文件，如 meobjsdt.dll（自动生成的木马程序动态库文件）。

接着，利用启动盘进入 DOS，在提示符后输入“del d:\windows\system32\meobjsdt.dll”，按回车键，即可将 meobjsdt.dll 文件删除（这里以删除 meobjsdt.dll 文件为例）。

最后，重新启动系统即可。

案例 29 在 DOS 中，不能识别 NTFS 文件系统分区怎么办

在 Windows 2000/XP/2003 下，NTFS 文件系统的分区是可以识别的，但在纯 DOS 下却不能识别。图 4-14 所示的是利用 fdisk 来查看 NTFS 文件系统的分区。这是因为在 DOS 下，只支持 FAT、FAT16、FAT32 格式的文件系统。

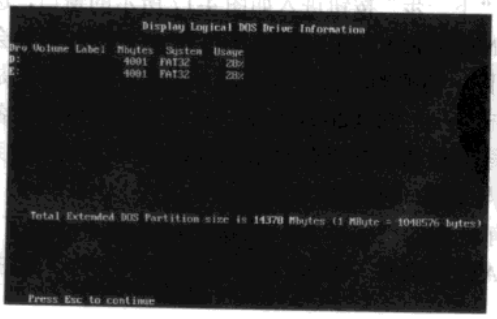


图 4-14

在通常情况下，读者需要进入 DOS 对硬盘进行重新分区、格式化，以及系统的安装/重装、系统的维护等操作。如果系统盘是 NTFS 文件系统，那么将无法在 DOS 下对系统盘进行

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

格式化，并重新安装系统。这时就需要借助第三方工具——NTFSDOS PRO 在 DOS 下识别和访问 NTFS 文件系统的分区。

要在 DOS 下使用 NTFSDOS PRO 工具识别 NTFS 文件系统，必须要通过以下的操作来实现。

1. 在 Windows 2000/XP/2003 系统中安装 NTFSDOS PRO

读者可以从华军软件园、PCHome 等网站下载 NTFSDOS PRO 汉化版，下载后必须先在 Windows 2000/XP/2003 系统下进行安装。具体的安装操作，根据向导提示完成即可。

2. 制作在 DOS 下运行的 NTFSPRO 程序

NTFSDOS PRO 汉化版安装完成后，就可以制作在 DOS 下运行的 NTFSPRO 程序。先运行“NTFSDOS 启动盘制作向导”，进入制作向导界面，如图 4-15 所示。

一直单击“下一步”按钮（前几步采用默认设置即可），直到进入到图 4-16 所示的界面，选择系统的安装目录，如 C:\WINDOWS、D:\WINDOWS（Windows XP 系统），或是 C:\WINNT、D:\WINNT（Windows 2000/2003 系统）。

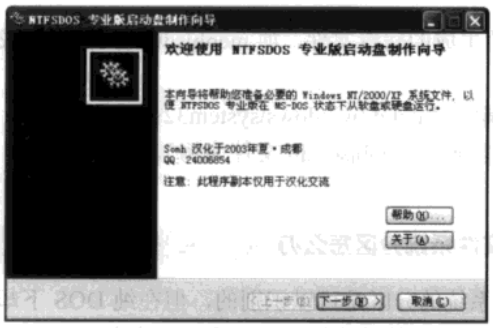


图 4-15

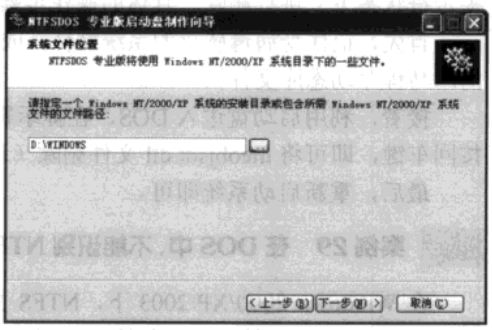


图 4-16

设置完成后，单击“下一步”按钮进入如图 4-17 所示的窗口，选择一个目录用于保存制作的在 DOS 下运行的 NTFSPRO 程序。若是保存到 A 盘中，向导会向软盘上传输制作完成的文件。根据情况的不同，需要的软盘可能会是 2 张或 3 张。如果是 Windows XP 系统，会需要 3 张盘；如果是 Windows 2000/2003 系统，则需要 2 张盘。准备好 3 张空白软盘后，单击“下一步”按钮，向导会自动压缩所有的 Windows 2000/XP/2003 系统文件，并拷贝到软盘上。在制作过程中，向导会提示重新插入空白软盘。

如果用户手中没有足够的空白软盘，或手中已经有启动盘了，可以将制作成的文件直接保存到硬盘中 FAT32 文件系统的分区中。在本例中，直接将制作的文件保存到 D:\NTFSPRO 中。

单击“下一步”按钮，开始向 D:\NTFSPRO 中压缩所有 Windows 2000/XP/2003 的系统文件和生成的 NTFSPRO.EXE、NTFSCHK.EXE 等文件。输入完成后，进入图 4-18 所示的窗口，单击“完成”按钮结束向导。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

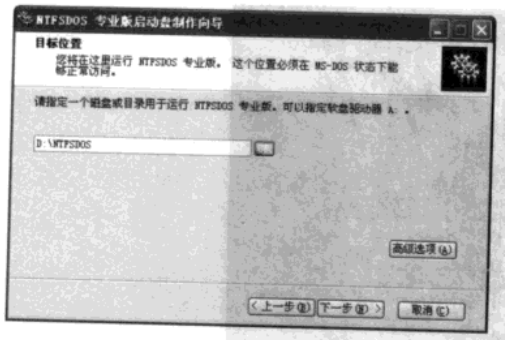


图 4-17

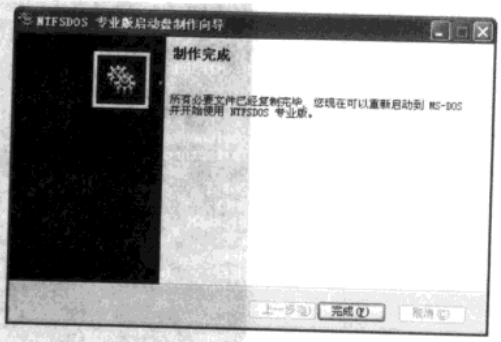


图 4-18

3. 进入 DOS 下，运行 NTFSPRO 程序来识别 NTFS 文件系统

用启动盘进入 DOS，在 DOS 中进入 NTFSPRO 文件所在的磁盘目录，接着在提示符后输入“dir”，按回车键即可显示 NTFSPRO.EXE、NTFSCHK.EXE 等文件，如图 4-19 所示。

这时，在提示符后输入“ntfspro”，按回车键即可开始对磁盘进行全部扫描，扫描硬盘中有没有 NTFS 分区格式。扫描后，它会自动对所有的 NTFS 分区进行装载，并给每个分区分配一个惟一对应的盘符。本例中利用 NTFSPRO 扫描到 1 个 NTFS 分区（Windows 2000/XP/2003 系统下是 F 盘），并分配“G:”为对应的盘符，如图 4-20 所示。

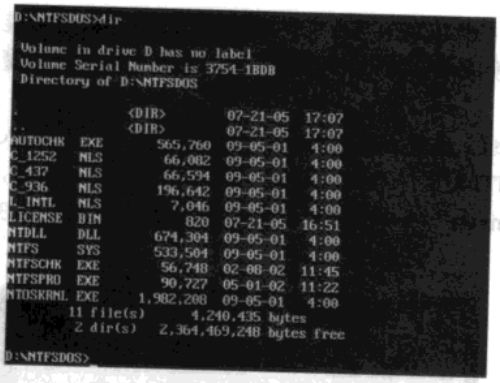


图 4-19

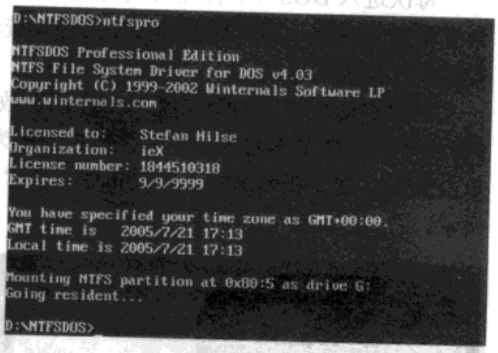


图 4-20

接着用户在提示符后输入“g:”，按回车键进入 G 盘根目录。然后在提示符后输入“dir”，按回车键即可以看到 G 盘中所有的文件，如图 4-21 所示。

接下来可以对该盘符中的目录、文件进行操作，也就是对 F 盘进行操作，所有的操作都是有效的。

制作的 NTFSDOS 启动盘或保存在磁盘中的 NTFSPRO，最好保存好。当退出此次操作后，下次再进入 DOS，还需要运行 NTFSPRO.EXE，才可以重新扫描 NTFS 分区，并分配对应磁盘。当然如果 NTFSPRO 文件丢失、损坏，重新制作即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
Mounting NTFS partition at 0x80:5 as drive G:
Going resident...

D:\NTFSDOS>g:

G:\>dir

 Volume in drive G is
 Directory of G:\

267-1          <DIR>          07-21-05   3:47 267-1
BACK           <DIR>          07-14-05  15:52 BACK
DISKGEN  EXE       142,244  03-22-05  14:46 diskgen.exe
F32      COM        21,204  10-31-03  11:11 f32.com
HELP           <DIR>          07-21-05   3:47 help
HELP     HLP         8,934  03-20-05  15:04 HELP.HLP
PCT90          <DIR>          07-21-05   3:46 PCT90
TOOLS          <DIR>          07-21-05   3:46 TOOLS
WIN98          <DIR>          07-14-05  17:41 WIN98
WITREN         <DIR>          07-14-05  15:52 WITREN
       3 file(s)        172,382 bytes
       7 dir(s)       6,312.75 MB free

G:\>
```

图 4-21

案例 30　如何利用 PM（分区魔术师）将 NTFS 文件系统转换为 FAT32 文件系统

注意　尽管使用 PM（分区魔术师）可以把 NTFS 分区转化为 FAT32 文件系统，并最大限度地保留 NTFS 格式分区上的原有数据。但是由于分区魔术师不支持中文文件名，所以事先一定要记住把 NTFS 格式分区里的中文文件、目录名都改成英文名字，这样才能确保 NTFS 分区的正确转换，否则该分区中所有以中文命令的文件和目录都将无法打开。

每次进入 DOS 中，都需要利用 NTFSDOS 才能识别 NTFS 文件系统，这样有些读者可能会感觉比较麻烦。如果想将 NTFS 文件系统转换成 FAT32 文件系统，可以利用 PM（分区魔术师）工具来实现。

利用启动盘进入 DOS，进入 PM 的存放目录，在提示符后输入“pqmagic”，按回车进入 PM 主界面。在主界面中，可以看到 F 分区为 NTFS 文件系统，如图 4-22 所示。选中 F 分区，单击鼠标右键，在弹出的下拉菜单中单击“Convert”→“NTFS to FAT32”命令，如图 4-23 所示。

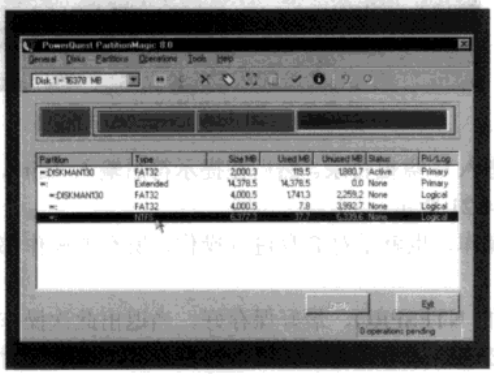


图 4-22

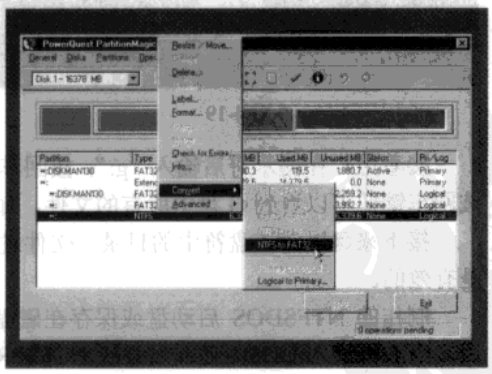


图 4-23

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这时，弹出图 4-24 所示的提示窗口，询问是否进入转换。单击“OK”按钮会弹出警告信息，警告在转换后会带来的负面影响，如在转换后会丢失文件等，如图 4-25 所示。根据笔者多次测试，转换后一般不会发生文件丢失的情况。

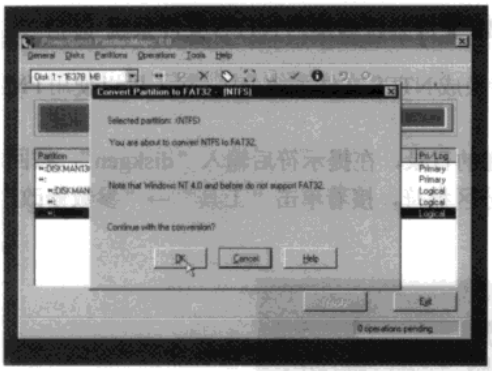


图 4-24

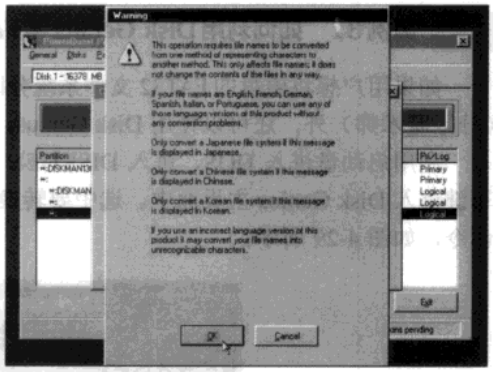


图 4-25

单击“OK”按钮后，即可将 NTFS 文件系统转换成 FAT32 文件系统，如图 4-26 所示。单击“Apply”按钮确认所做的转换，此时会弹出图 4-27 所示的提示窗口，单击“Yes”按钮开始保存设置，如图 4-28 所示。

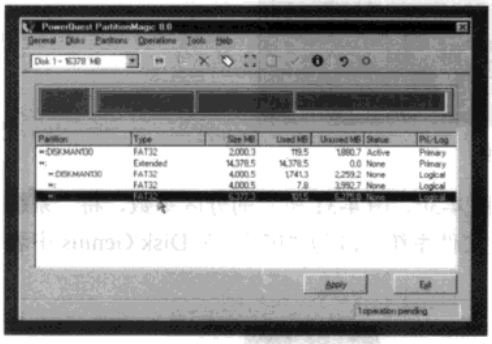


图 4-26



图 4-27

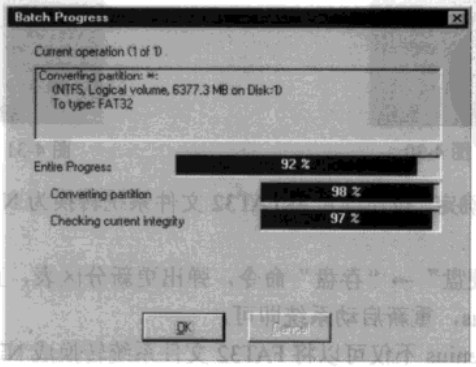


图 4-28

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

更新完成后，单击“Exit”按钮退出 PM，重新启动系统即可。

在 DOS 下，PM 不仅可以将 NTFS 文件系统转换成 FAT32 文件系统，也可以将 FAT32 文件系统转换成 NTFS 文件系统。

案例 31　如何利用 Disk Genius 将 FAT32 文件系统转换为 NTFS 文件系统

如果用户想将磁盘的 FAT32 文件系统分区转换成 NTFS 文件系统分区，除了可以使用 PM（分区魔术师）外，还可以使用 Disk Genius。

利用启动盘进入 DOS，进入 DISKGEN 所在的目录，在提示符后输入“diskgen”，按回车键进入 Disk Genius 主界面中。选中要转换的分区盘符，接着单击“工具”→“参数修改”命令，如图 4-29 所示。

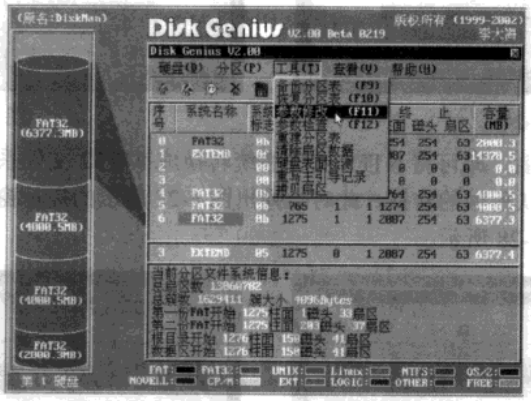


图 4-29

在弹出的“修改分区参数”对话框中，对照图 4-30、图 4-31 所示的分区参数，将“系统标志”中的“0b”（在 Disk Genius 中表示 FAT32 文件系统）改为“07”（在 Disk Genius 中表示 NTFS 文件系统）。

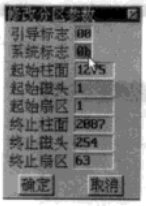


图 4-30



图 4-31

设置完成后，单击“确定”按钮即可将 FAT32 文件系统转换为 NTFS 文件系统，如图 4-32 所示。

转换过后，单击“硬盘”→“存盘”命令，弹出更新分区表，直接单击“确定”按钮。存盘后，退出 Disk Genius，重新启动系统即可。

在 DOS 下，Disk Genius 不仅可以将 FAT32 文件系统转换成 NTFS 文件系统，也可以将 NTFS 文件系统转换成 FAT32 文件系统。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

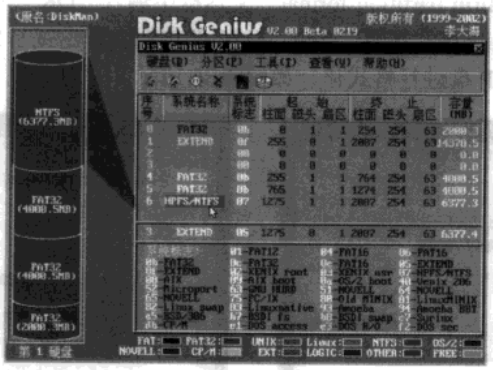


图 4-32

案例 32 在 DOS 下，如何对 NTFS 格式的分区的进行格式化

很多用户使用的都是 Windows XP 系统，一旦 Windows XP 遇到无法挽救的故障后，就需要重新安装系统。如果要直接在 DOS 下安装 Windows XP 系统，会自动将系统装入到 D 盘中，所以想要将系统装到 C 盘，就需要对 C 盘进行格式化。但是进入 DOS 后，却出现 C 盘无法识别的情况，这说明 C 盘为 NTFS 文件系统。那如何对 C 盘进行格式化呢？

遇到 C 盘是 NTFS 文件系统的情况，可以通过下面的方法对 NTFS 格式的分区进行格式化（这里以 F 盘的文件系统为 NTFS 为例）。

利用启动盘进入 DOS 下，运行 PM 进入主界面中。选中 F 盘，单击鼠标右键，从弹出的下拉菜单中单击“Format”命令，如图 4-33 所示。接着弹出如图 4-34 所示的窗口，若用户想在格式化时改变文件系统，可以在“Partition Type”下拉列表中进行选择。

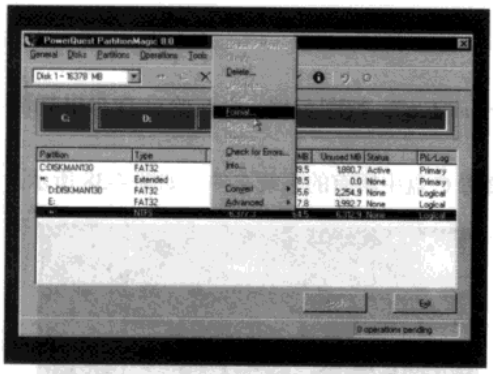


图 4-33

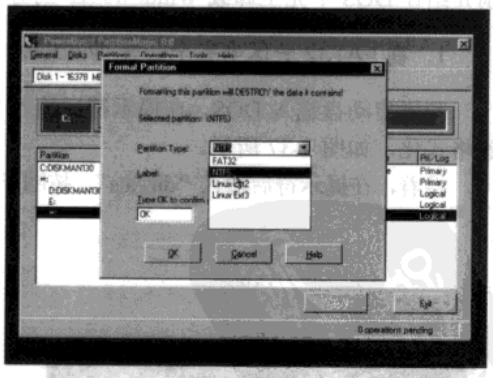


图 4-34

注意 如果用户是对C盘的NTFS文件系统进行格式化，可以在图4-34所示的界面中，将“Partition Type”设置为“FAT32”文件系统。在重新安装 Windows XP 时，再将 C 盘转换为 NTFS 文件系统。否则在 DOS 下安装 Windows XP 时将无法识别 C 盘。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在“Type OK to confirm partition format”文本框中输入“OK”后，单击“OK”按钮完成格式化的设置操作。返回到主界面，单击“Apply”按钮会弹出提示信息（如图 4-35 所示），单击“Yes”按钮开始对 F 盘进行格式化，如图 4-36 所示。

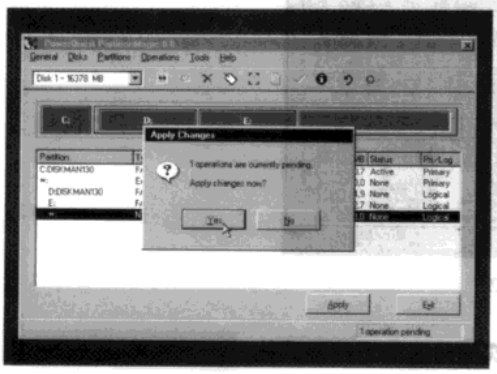


图 4-35

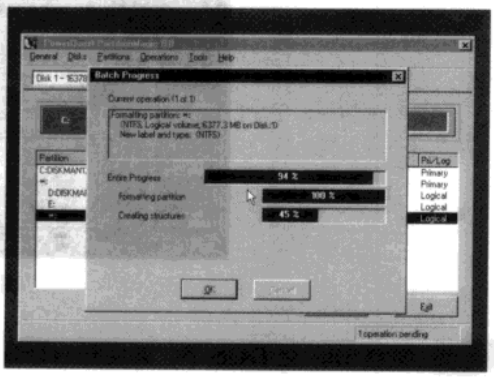


图 4-36

操作完成后，在弹出的窗口中单击“OK”按钮返回到主界面中。单击“Exit”按钮退出 PM，并重新启动系统即可。

案例 33　如何完全卸载多操作系统中的 Windows XP

Windows 98 和 Windows XP 共存是多操作系统中的经典共存方案，而要删除 Windows XP 系统，则不只是对安装 Windows XP 的系统盘进行格式化就完事了。要完全卸载 Windows XP，除了格式化系统所在的盘符外，还需要删除多操作系统启动菜单和多余的系统文件。并且还要注意 Windows XP 系统盘所使用的文件系统是 FAT32，还是 NTFS。下面就这两种情况，分别介绍在 DOS 下完全卸载 Windows XP 的方法。

1. 在 FAT32 分区中完全卸载 Windows XP

利用启动盘进入 DOS，在提示符后输入“format d:/q”，按回车键，便开始对 D 盘进行快速格式化，如图 4-37 所示。

接着，在提示符后输入“dir /a:s”，按回车键查看 C 盘中所有的系统文件，如图 4-38 所示。

```
A:\>format d:/q

WARNING, ALL DATA ON NON-REMOVABLE DISK
DRIVE D: WILL BE LOST!
Proceed with Format (Y/N)?y

Checking existing disk format.
QuickFormatting 4,000.53M
Recording current bad clusters
 55 percent completed.
```

图 4-37

```
C:\>dir/a:s

 Volume in drive C has no label
 Volume Serial Number is 3754-1BDB
 Directory of C:\

BOOTSECT DOS          512  07-12-05  15:27
NTLDR             229,536  09-05-01  12:00
BOOTFONT BIN      322,730  09-05-01  12:00
NTDETECT COM       45,124  09-05-01  12:00
BOOT     INI          194  07-12-05  17:27
PAGEFILE SYS   120,586,240  07-12-05  16:50
CONFIG   SYS            0  07-12-05  17:49
IO       SYS            0  07-12-05  17:49
MSDOS    SYS            0  07-12-05  17:49
SYSTEM~1       <DIR>       07-12-05  18:00
       9 file(s)    121,184,336 bytes
       1 dir(s)   1,972,080,640 bytes free

C:\>
```

图 4-38

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

注意 若只输入“dir”，将无法查看 C 盘中的系统文件，即 boot.ini、bootfont.bin、bootsect.dos、ntdetect.com、pagefile.sys 等系统文件无法显示。所以必须“dir”后加上参数“/a:s”。

然后，利用 deltree 命令删除 Windows XP 在 C 盘所留下的文件。这只需在提示符后依次输入以下指令，并按回车键，再按“Y”键即可，如图 4-39 所示。

- deltree C:\boot.ini
- deltree C:\bootfont.bin
- deltree C:\bootsect.dos
- deltree C:\ntdetect.com
- deltree C:\pagefile.sys

注意 使用 del 命令将无法删除删除这 5 个文件。当使用 del 来删除这 5 个文件时，会提示“File not found”（文件不存在）的错误信息。若读者要使用 del 命令来删除这 5 个系统文件，必须在删除之前利用 attrib 命令去掉这 5 个文件的系统属性和隐藏属性，指令分别为“attrib boot.ini –s –h”、“attrib bootfont.bin –s –h”、“attrib bootsect.dos –s –h”、“attrib ntdetect.com –s –h”和“attrib pagefile.sys –s –h”，修改属性后再用 del 命令即可进行删除。

删除完成后，需要在提示符后输入“sys c”，按回车键向 Windows 98 系统盘传送 command.com 文件。

最后，在提示符后输入“fdisk /mbr”，按回车键恢复主引导记录，如图 4-40 所示。如果不修复主引导记录，默认情况下会识别成 Windows XP 依然存在，可能会引起系统错误。

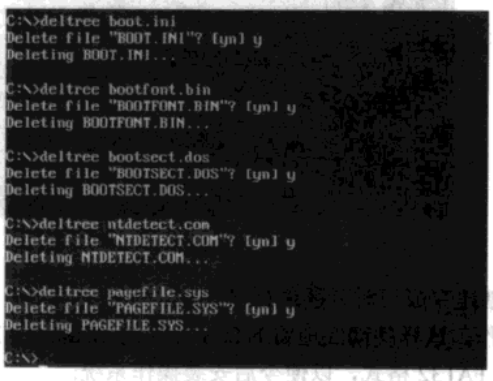


图 4-39

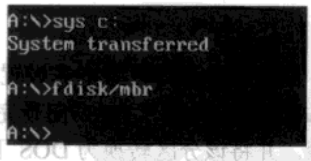


图 4-40

2. 在 NTFS 分区中完全卸载 Windows XP

要在 DOS 下完全卸载 NTFS 分区中的 Windows XP 系统，会比较麻烦一点。因为 DOS 不能识别 NTFS 系统，所以要卸载 Windows XP 就需要借助一些工具来实现。虽然有些读者使用 fdisk 来删除，但是这会破坏硬盘中的数据（甚至是毁灭性的），所以笔者不建议使用

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

FDISK。这里推荐使用 PM、Disk Genius 或 Windows XP 安装光盘中的“故障恢复控制台”来删除。

小知识

虽然 fdisk 命令也无法识别 NTFS 分区，但是可以将 NTFS 分区转换为未知分区（Non-DOS Partition）。进入 fdisk 界面，选择“3. Delete partition or Logical DOS Drive”→“4. Delete Non-DOS Partition”，会提示是否真的要删除该分区，按“Y”键确认，NTFS 分区就被删除了。

（1）利用 PM（分区魔术师）、Disk Genius 格式化 NTFS 分区

在 DOS 下，PM 和 Disk Genius 是可以识别 NTFS 分区的，而且 PM 可以直接对 NTFS 分区进行格式化，Disk Genius 可以直接删除 NTFS 分区再重新创建。这两个工具都能达到格式化 NTFS 分区的目的。利用这两个工具所执行的操作只对当前盘起作用，并不会影响或破坏其他分区中的数据。

关于如何使用 PM（分区魔术师）格式化 NTFS 分区，并在格式化时将分区转换为 FAT32 格式，在上面的案例中已经介绍，可以查看。下面具体介绍使用 Disk Genius 删除 NTFS 分区，并重新创建该分区的操作方法。

利用启动盘进入 DOS，进入 Disk Genius 的存放目录，运行 diskgen 进入主界面。先选中 NTFS 格式的 Windows XP 分区，单击“分区”→“删除分区”命令，将 NTFS 分区删除，如图 4-41 所示。接着单击“分区”→“新建分区”命令，重新创建分区，如图 4-42 所示。



图 4-41

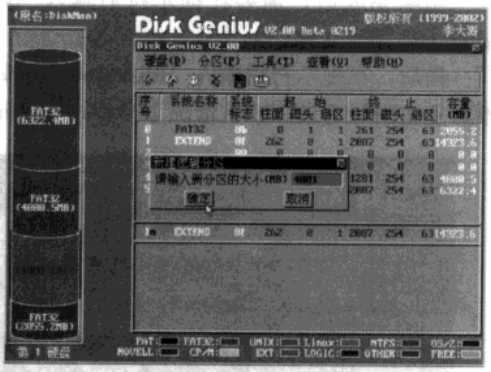


图 4-42

创建时将该分区的格式设置为 FAT32，创建完成后对分区进行格式化。单击“工具”→“格式化 FAT 分区”，根据向导完成格式化操作。这样就彻底地将 NTFS 分区的 Windows XP 删除，并将该分区转换为 DOS 下可以识别的 FAT32 格式，以便今后安装操作系统。

其实，也可以利用 PM 和 Disk Genius 将 NTFS 分区转换为 FAT32 分区，再对其进行格式化操作，效果是一样的，这里就不再介绍。

（2）利用 Windows XP 安装光盘中的“故障恢复控制台”来格式化 Windows XP 分区

在 Windows XP 的安装光盘中有个特别的工具——故障恢复控制台，在 Windows XP 出现故障或崩溃后，可以用它来修复系统。也可以利用该工具来格式化 NTFS 格式的 Windows XP 分区。本书后面有一章来专门介绍“故障恢复控制台”的安装和使用，这里只是大致地

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

介绍一下操作步骤，具体的操作请参考第 7 章的内容。

第一步，将 Windows XP 的安装光盘放入光驱中，运行后进入欢迎屏幕时，按“R”键进行修复页面，再按“C”键进入“故障恢复控制台”中。

第二步，进入故障恢复控制台后，假设 NTFS 格式的 Windows XP 分区是 D 盘，则在提示符后输入“format d:/q”，按回车键，接着提示是否格式化 D 盘。输入“y”，按回车键使开始快速格式化 D 盘。

小知识

其实，还可以使用 NTFSDOS 程序，在 DOS 下识别 NTFS 分区，然后利用 format 命令来格式化分区。不过这样操作有点复杂，有兴趣的读者可以自己研究。

任选一种方法格式化 NTFS 格式的 Windows XP 分区，接下来进入 DOS，再使用 deltree 删除 boot.ini、bootfont.bin、bootsect.dos、ntdetect.com、pagefile.sys 等系统文件。删除完这些文件，在提示符后输入“sys c:”，按回车键向 Windows 98 系统盘传送 command.com 文件。

最后，在提示符后输入“fdisk /mbr”，按回车键恢复主引导记录。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第5章 DOS下的经典应用案例

在Windows“诞生”之前，DOS是应用非常广泛的操作系统；而当Windows普及后，DOS却在底层“默默地”为Windows系统解决各种疑难杂症。所以在DOS的下一些经典应用一直被使用。

案例34 使用dir命令查看目录中的文件时，屏幕滚动太快看不清楚内容怎么办

dir是directory（目录）的缩写，该命令的作用是显示当前目录下的全部或部分文件或子目录，是DOS下使用频率最高的命令之一。有些读者在DOS下查看某一目录下的文件时，直接在提示符后输入“dir”后按回车键，若当前目录下有很多文件或子目录，会发现内容还没有看清楚就已经滚动上去了。遇到这样的情况，就需要使用dir命令的参数。

1. 认识dir命令格式

```
命令格式:dir[<盘符>][<路径>][<文件名>][<扩展名>][/p][/w][/s][/a[:]属性][/o[:]排序方式]
```

参数说明如下。

- /p：显示一屏后自动暂停，按任意键继续。
- /w：每行只显示5个文件名和扩展名。
- /s：列出指定目录和其下属各级子目录中的所有文件。
- /a:[属性]：显示具有指定属性的文件或者目录。若未指定属性，则显示除隐藏文件和系统文件以外的所有文件。

属性开关

h：显示隐藏文件。
s：显示系统文件。
d：显示目录。
-d：仅显示文件。
r：显示只读文件。
-r：显示非只读文件。

注意 属性开关可以组合使用，但属性之间不能用空格分开。

- /o:[排序方式]：按指定的“排序方式”显示文件和目录。
- /q：显示文件所有者。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

排序方式

n：按文件名字母顺序排序。
d：按日期和时间的先后顺序排序。
s：按文件的大小排序，小的在前。
g：按目录在前、文件在后的顺序排序。

- /c：在文件大小中显示千位数分隔符，这是默认值。
- /-c：停用分隔符显示。

2. 利用 dir 分屏或分栏显示文件

如果要查看的目录下的文件或子目录过多，可以利用/p、/w 参数。

在 DOS 下的提示符后输入“dir /p”，按回车键，当显示满一屏时会自动暂停，并在屏幕的底端显示一行英文“Press any key to continue…”，意思是按任键继续，如图 5-1 所示。

在 DOS 下的提示符后输入“dir /w”，按回车键会以每行 5 个文件名和扩展名来显示，如图 5-2 所示。而使用用“/w”参数的弊端在于不能显示文件的大小和生成时间。

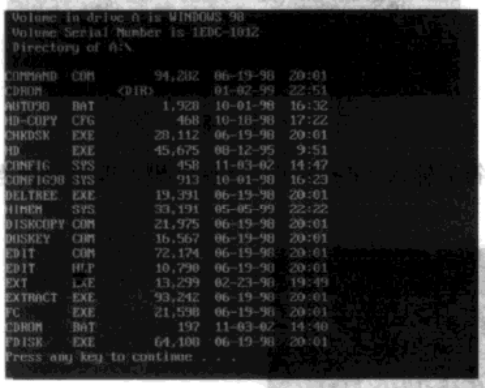


图 5-1



图 5-2

若要查看的目录下的文件和子目录非常多，可以在 DOS 下的提示符后输入“dir /w /p”，按回车键，这样每行只显示 5 个文件名和扩展名，并且在显示满一屏后自动暂停，如图 5-3 所示。

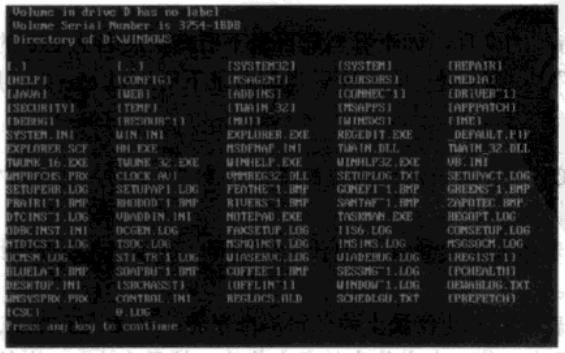


图 5-3

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3. 利用 dir 查看隐含文件、系统文件或特定文件

在 DOS 下的提示符后输入“dir”、“dir /p”、“dir /w”后按回车键，是无法查看目录中的隐藏文件和系统文件的。若要查看目录中的隐藏文件和系统文件，必须使用特定的参数。使用“/a: [属性]参数+属性开关”参数格式，就可以查看目录中的隐含文件、系统文件和只读文件。

在 DOS 下的提示符后输入“dir /a:h”，按回车键，就可以显示当前目录下的隐含文件，如图 5-4 所示。

在 DOS 下的提示符后输入“dir /a:s”，按回车键，就可以显示当前目录下的系统文件，如图 5-5 所示。

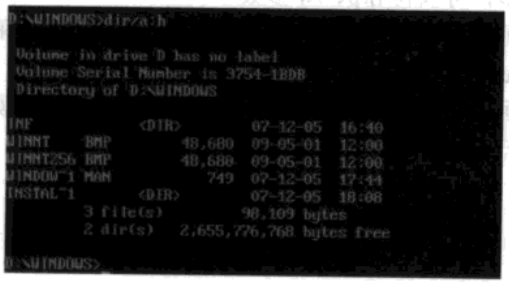


图 5-4



图 5-5

若只查看只读文件，可以在 DOS 下的提示符后输入“dir /a:r”，按回车键，即可显示当前目录下的只读文件，如图 5-6 所示。

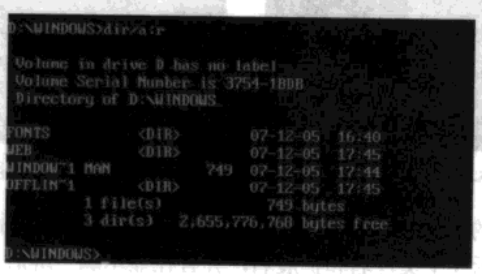


图 5-6

若用户只查看特定的文件，如查看当前目录下所有扩展名为 exe 的文件，就可以在提示符后输入“dir *.exe”，按回车键，即可查看当前目录下所有以 exe 为扩展名的文件，如图 5-7 所示。

小知识

在 DOS 下经常使用两种通配符：一是“*”，另一个是“?”。它们的作用分别如下。

“*”表示其所处位置上的任一字符串。例如 b*.*，表示以 b 为开头的所有文件。

“?”表示其所处位置上的任何一个字符。例如 abc?.bat，表示当前目录下以 abc 开头，第 4 个字符为任意字符的、扩展名为 bat 的所有文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

案例 35 在 DOS 下如何利用相对路径、绝对路径来创建或删除目录

在 Windows 下的“我的电脑”窗口中可以单击“文件”→“新建”→“文件夹”命令来创建文件夹（在 DOS 里称为目录），而选中某一个文件夹单击“文件”→“删除”命令则删除该文件夹，那么在 DOS 下是如何创建和删除目录呢？这时就需要用到 md 和 rd 命令。

1. 认识 md、rd 命令格式

```
命令格式：md [盘符:][路径][子目录名]
命令格式：rd [盘符:][路径][子目录名]
```

说明：这里“路径”既可以使用相对路径，也可以使用绝对路径。用相对路径建立当前目录的下一级子目录比较方便；而用绝对路径建立其他盘符中的目录比较方便。

2. 利用相对路径、绝对路径来创建、删除目录

下面介绍如何利用相对路径、绝对路径来创建和删除目录。

（1）利用相对路径、绝对路径来创建目录

在 DOS 下，如用户想在 E 盘根目录创建名为“back”目录，即可在提示符后输入“md e:\back”，铵回车键，接着用 cd 命令进入 E 盘根目录，利用 dir 命令即可看到创建的“back”目录，如图 5-8 所示。

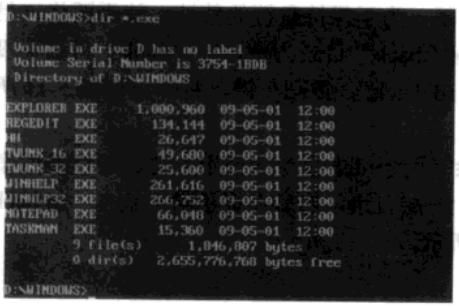


图 5-7

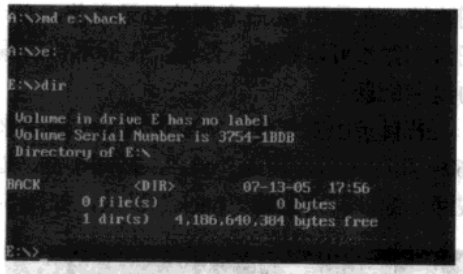


图 5-8

以上是利用绝对路径来创建“back”目录，利用相对路径也可以创建。只不过先要进入 E 盘根目录，在提示符后输入“md back”，按回车键，即可创建“back”目录。

小知识

当“back”目录创建好后，利用 cd 命令进入“back”目录，会发现目录中多了 2 个目录，分别是“.”和“..”，如图 5-9 所示。刚刚建立的目录，按常理来说这个目录中应该什么都没有的，怎么多了两个目录呢？

其实，在 DOS 下建立任何目录，这个“.”和“..”都会在目录中出现。因为“.”代表此目录本身，而“..”代表此目录的上一层目录。显然，一个目录既然已经存在了，就不可能没有自身，也不可能没有上一层目录。

在“back”目录下，输入“cd..”，按回车键，可以返回到上一导目录，如图 5-10 所示。只有返回到“back”上一层目录才可以删除“back”目录。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

利用上面的方法，可以随意地当前目录创建新的子目录，或利用绝对路径创建在其他盘符下的子目录。不过，在创建的时候要注意以下两个问题。

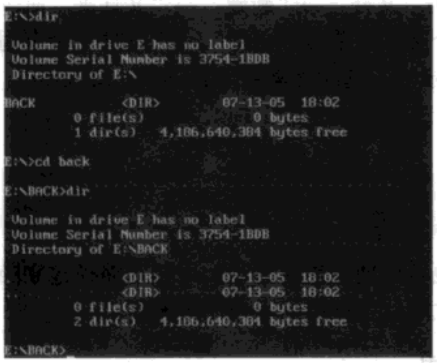


图 5-9

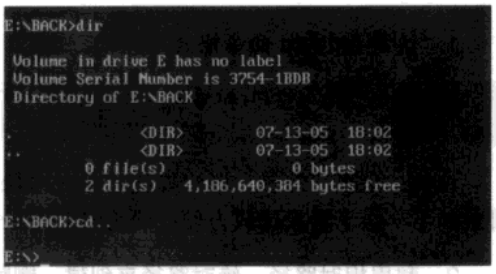


图 5-10

- 在同一个磁盘的同一级目录下，不允许创建同名的子目录。但是，在不同的目录中，可以创建同名的子目录。
- 只要磁盘的可用空间允许，可以创建任意多级的子目录，但是最长的路径（包括“\”在内）不得超过 63 个字符。

（2）利用相对路径、绝对路径来删除目录

假若上面创建的“back”目录，现在不需要了，为了保持盘符的整洁，就需要将该目录删除掉。在使用 rd 命令删除目录之前，必须确保“back”目录为空，即“back”目录下没有任何文件才可以删除；否则，在提示符后输入“rd back”，按回车键，将弹出如图 5-11 所示的提示信息。

若目录中有文件，需要使用 del 命令来删除（关于 del 命令的使用方法，可以参照案例 36）。删除过后，输入“cd..”，按回车键，返回上一层目录。然后在提示符后输入“rd back”，按回车键，即可删除“back”目录，如图 5-12 所示。

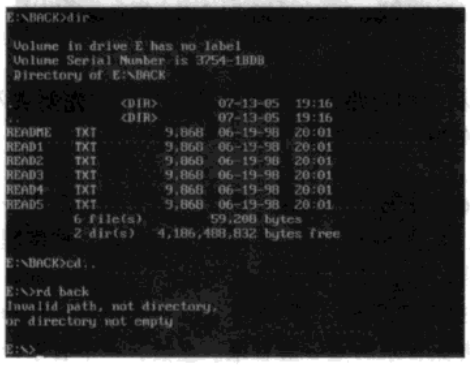


图 5-11

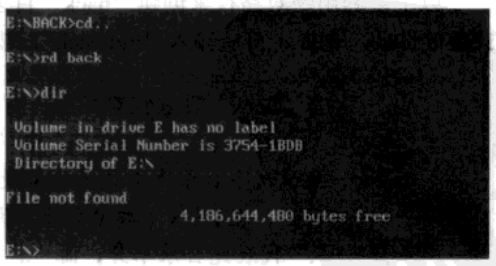


图 5-12

上面是使用相对路径来删除“back”目录，如果当前提示符为“A:\>”，而且也确保“back”目录中没有任何文件，就可以利用绝对路径来删除“back”目录。在“A:\>”后输入“rd e:\back”，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

按回车键，即可删除“back”目录。

小知识

如果利用 deltree /y 命令，即使“back”目录中有文件，也可以将“back”目录删除（关于 deltree 命令的使用方法，可以参考案例 36）。

而在 Windows 2000/XP/2003 的命令提示符下，rd 命令增加了/s、/q 参数。/s 参数：用于删除指定目录下的子目录和文件，可以用于删除目录树，相当于 deltree /y 命令。/q 参数：表示安静模式，删除目录树时将不再提示确认。

利用上面的方法，可以删除其他无用的目录。不过，在删除目录时要注意以下问题。

- 如果子目录下有文件，要把该子目录下的文件先用 del 命令全部删除才可删除这个子目录。
- 根目录不能被删除。
- 如果子目录是当前目录，要退回到根目录或其他目录，才可以删除子目录。
- 如果子目录下有子目录，要先删除一个路径中的最下一级子目录，再由下向上逐级删除。

案例 36 在 DOS 下如何删除垃圾文件和垃圾目录

在上面的案例中，已经提到利用 del 命令来删除子目录下的所有文件，这即为此命令的功能所在。而 deltree 命令是 del 命令的超级加强版，它不仅可以删除文件，并且会将指定目录和其下的所有文件和子目录一并删掉。在 DOS 下，若发现一些无用文件或无用目录，就需要利用这 2 个命令来删除。

1. 认识 del、deltree 命令格式

```
命令格式：DEL [盘符:][路径]〈文件名〉[/p] [/f] [/s] [/q] [/a:[属性]]
```

参数说明如下。

- /p：删除每一个文件之前提示确认信息
- /f：强制删除只读文件
- /s：从所有子目录删除指定文件
- /q：安静模式。删除全域通配字符时，不要求确认
- /a:[属性]：根据属性选择要删除的文件

属性开关

h：隐含文件。
s：系统文件。
a：存档文件。
r：只读文件。

```
命令格式：deltree[盘符:][路径]〈文件名〉[/y]
```

参数说明如下。

- /y：在删除时不弹出提示信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

注意

deltree 是外部命令，必须拷贝到 DOS 中才能使用该命令。不过在 DOS 启动盘中，该命令已经存在，所以不需要再拷贝到 DOS 中。

而上面所讲到的 dir、md、rd、del 命令，都是内部命令。这些命令驻留在内存中，可以直接使用，而外部命令必须拷贝到当前目录下才可以使用。

2. 利用 del、deltree 删除垃圾文件和垃圾目录

若删除当前目录下指定的垃圾文件，如 read1.txt，可以在提示符后输入“del read1.txt”，按回车键，即可删除 read1.txt 文件，如图 5-13 所示。

若当前目录下的文件都是无用的垃圾文件，可以在提示符后输入“del *.*”，按回车键，系统会提示是否删除目录下的所有文件。输入“y”，按回车键即可删除目录下所有的文件，如图 5-14 所示。

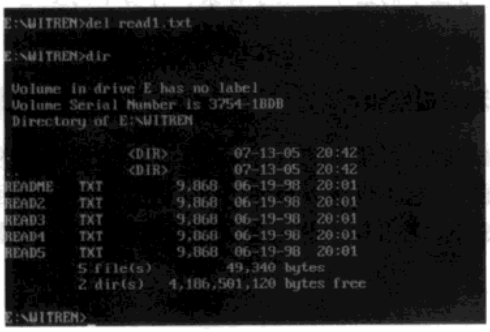


图 5-13

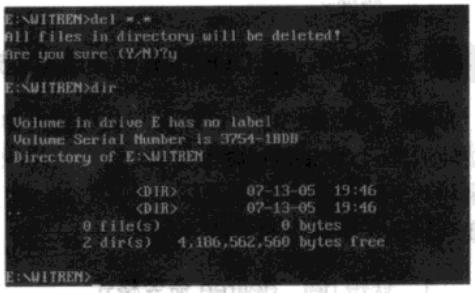


图 5-14

若想一次性删除图 5-14 所示的“witren”目录，以及该目录下所有的子目录和文件。利用 del 命令实现起来比较麻烦，此时就可以利用 deltree 命令来一次完成全部的删除操作。

要实现一次性删除操作，首先要回到启动盘符下，或回到某个盘符下具有 deltree 命令的目录中。接着在提示符后输入“deltree e:\witren”，按回车键，提示用户是否删除该目录以及目录下所有的子目录和文件，如图 5-15 所示。输入“y”，按回车键即可删除“witren”目录，如图 5-16 所示。



图 5-15



图 5-16

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在利用 del 和 deltree 命令删除文件时，一定要慎重。如果真的误删除了某些重要的文件，可以利用 undelete 命令来进行恢复。

案例 37 在 DOS 下如何来更改文件名

在 Windows 系统下若要对文件进行更名，只需要选中文件，单击“文件”→“重命名”命令，输入更改后的文件名即可。而在 DOS 下为文件更名，就需要利用 copy 和 ren 命令来实现。

1. 认识 copy、ren 命令格式

命令格式：copy<源文件名>[<目标文件名>]

功能说明如下。

将由<源文件名>所指定的一个文件或一类文件拷贝到<目标文件名>下，同时也可以进行更名。拷贝后<源文件名>的内容不变。

命令格式：ren<旧文件名><新文件名>

功能说明如下。

- 将<旧文件名>所指定的文件改变为<新文件名>所指定的文件名称。更改后旧文件名消失，新文件名列于磁盘目录中，内容不变。
- <旧文件名>所指定的文件必须是磁盘上已存在的文件，而<新文件名>必须在该磁盘上不存在，否则就无法执行，且有错误信息返回。
- <旧文件名>中使用通配符，则<新文件名>相对应的位置处也要使用对应的通配符。

2. 利用 copy、ren 命令为文件更名

下面介绍如何使用 copy、ren 命令为文件更名。

（1）利用 copy 命令来为文件更名

如要将 e:\back 目录中的 read.txt 文件更名为 data.txt 文件，可以在“E:\BACK>”提示符后输入“copy read.txt data.txt”，按回车键，即可将 read.txt 文件重新更名为 data.txt 并保存在 e:\back 目录中，如图 5-17 所示。而原 read.txt 文件不变，接着使用 del 命令将 read.txt 文件删除，这样即可将 read.txt 文件更名为 data.txt。

（2）利用 ren 命令来为文件更名

虽然使用 copy 命令可以更改一些文件名，但是 copy 命令只能对文本文件（txt）和数据文件（bak、dat）进行改名。若要对其他文件进行更名，必须使用 DOS 中专门的更名命令——ren。

若需要把 e:\back 目录中 data.txt 文件更名为 read.txt 文件，则可以在“E:\BACK>”提示符后输入“ren data.txt read.txt”，按回车键，即可将 data.txt 文件更名为 read.txt 文件，如图 5-18 所示。

注意 利用 ren 进行更名时，<旧文件名>与<新文件名>必须在同一目录下；否则不能更名，并给出出错信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

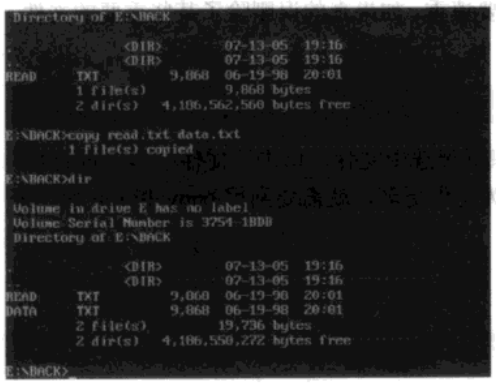


图 5-17

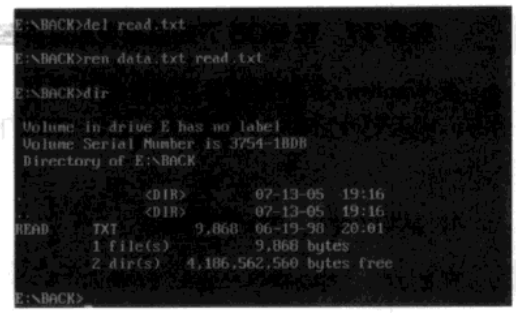


图 5-18

利用 ren 也可以成批更改多个具有相同扩展名的文件名，若将 e:\back 目录中所有以 txt 为扩展名的文件，更名为以 dat 为扩展名的文件。这时可以在提示符后输入“ren *.txt *.dat”，按回车键即可，如图 5-19（更名前）、图 5-20（更名后）所示。



图 5-19

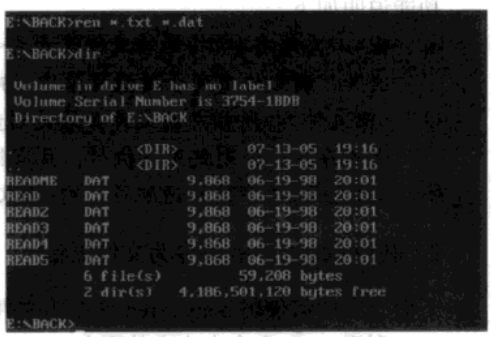


图 5-20

在使用 ren 命令为文件更名时，可以使用*和？通配符来成批更改多个相同的文件名，不过要注意相对位置的一致性。

案例 38 在 DOS 下如何改变文件的属性

文件属性主要分为 4 种，分别是只读属性、存档属性、隐含属性和系统属性。在 Windows 中只需要先选中文件，接着单击“文件”→“属性”命令进入“属性”对话框中；而在 DOS 下改变文件的属性，需要利用 attrib 命令来实现。

1. 认识 attrib 命令格式

```
命令格式：attrib [路径][文件名] [参数]
```

参数说明如下。

- +：添加文件属性。
- -：去除文件属性。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- r：只读属性。
- h：隐含属性。
- s：系统属性。
- a：存档属性。
- /s：显示目录下的所有文件属性。

2. 利用 ATTRIB 命令来改变文件的属性

若要改变文件的属性，先要查看目录中的文件属性。在提示符后输入“attrib /s”，按回车键，即可在屏幕中显示当前目录中所有文件的属性，如图 5-21 所示。也可以查看指定文件的属性，如在提示符后输入“attrib config.sys”，按回车键，即可查看 config.sys 文件的属性。

从图中可以看到 config.sys 文件只有存档属性，为了保证该文件的安全性，此时可以为 config.sys 文件添加系统属性、隐含属性。在提示符后输入“attrib +s +h config.sys”，按回车键，即可为 config.sys 添加系统属性、隐含属性，如图 5-22 所示。

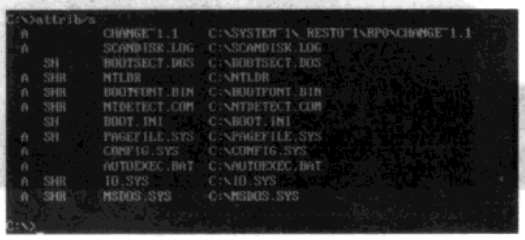


图 5-21

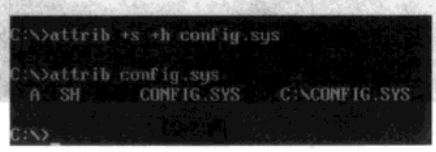


图 5-22

若要去除文件的属性，如 config.sys 的系统属性和隐藏属性，在提示符后输入“attrib -s -h config.sys”，按回车键即可。

案例 39 在 DOS 下如何对磁盘分区进行高级格式化

在利用 fdisk 对硬盘分区后，需要用到 format 对每个分区进行高级格式化。另外，安装了 windows XP 系统后，若系统崩溃要想重新安装系统，也必须使用格式化命令对系统盘进行高级格式化。否则，系统会自动安装到下一个盘符中。

1. 认识 format 命令

命令格式：format[<盘符 1>] [/s] [/v: <卷标] [/q] [/f:size] [/u] [/c]

参数说明如下。

- /s：格式化后，并将系统引导文件拷贝到该磁盘中。
- /v:label：格式化后，为该磁盘指定卷标。
- /q：快速格式化，只是删除格式化过的磁盘的文件分配表和根目录，而不检查磁盘上的坏扇区。
- /f:[size]：指定被格式化的软盘容量，推荐使用默认设置。
- /u：完全格式化，格式化后不能用 unformat 命令来恢复。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- /c：重新测试磁盘坏簇。
- /t:tracks：为磁盘指定每面磁道数。
- /n:sectors：指定每条磁道的扇区数。
- /1：格式化单面软盘。
- /4：在高密度驱动器内格式化 5.25 寸容量为 360KB 的软盘。
- /8：每条磁道格式化八个扇区。

2．利用 format 命令对磁盘分区进行高级格式化

若这里要对 D 盘进行高级格式化，只需要在提示符后输入 format d: /q<回车>，接着提示是否对该分区进行高级格式化信息，如图 5-23 所示。

在提示信息后输入“y”，按回车键，开始对 D 盘进行快速格式化（因为是已经格式化过的分区，这里就可以使用快速格式化参数），如图 5-24 所示。

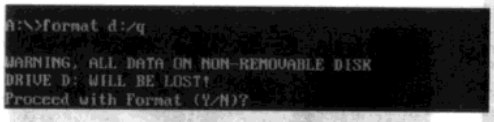


图 5-23

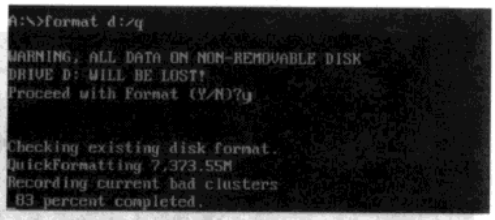


图 5-24

当格式化完成后，提示如图 5-25 所示的信息。按回车键，对格式化的磁盘盘符建立卷标，如图 5-26 所示。这样对 D 盘的高级格式化操作顺利结束。

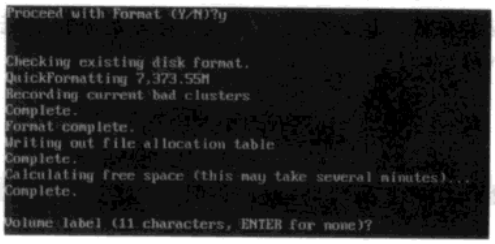


图 5-25

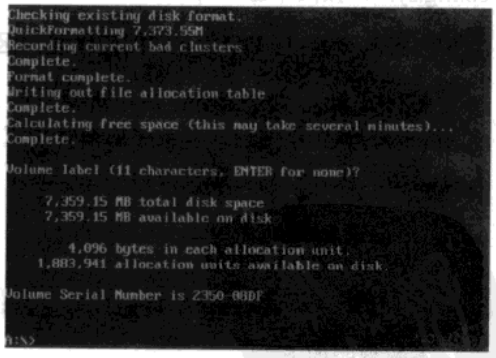


图 5-26

案例 40　在 DOS 下忘记了某命令的基本格式和参数怎么办

DOS 下的内外部命令很多，作为初学者来说很难一下子记清这么多的命令，以及命令的基本格式和参数。那么在使用某个命令时，如果不了解或忘记了该命令的基本格式和参数怎么办？此时可以利用以下方法来解决。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1. 在 DOS 命令后面加“/? ”，以查看该命令的详细信息

若要知道 smartdrv 命令的基本格式和参数，可以在提示符后输入“smartdrv/?”，按回车键，即在屏幕中显示该命令的基本格式和参数说明，如图 5-27 所示。

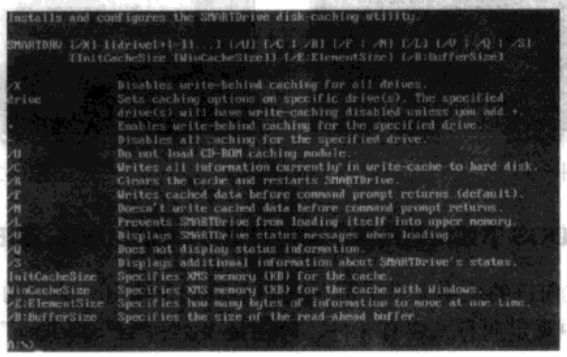


图 5-27

2. 利用 help 命令来查看 DOS 命令的详细信息

若用户只大致记得某个命令，可以在提示符后输入“help”，按回车键，屏幕上即可显示 DOS 下的所有命令，如图 5-28 所示。

将光标移至需查询的命令上，按回车键可查询到其语法格式，比如移至 cd 命令，如图 5-29 所示。

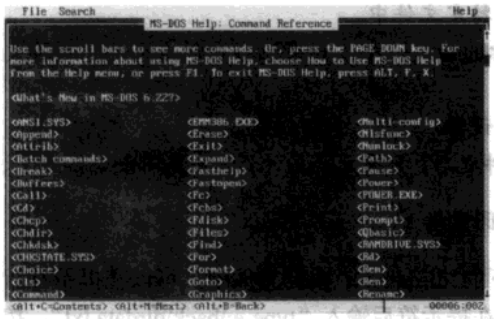


图 5-28

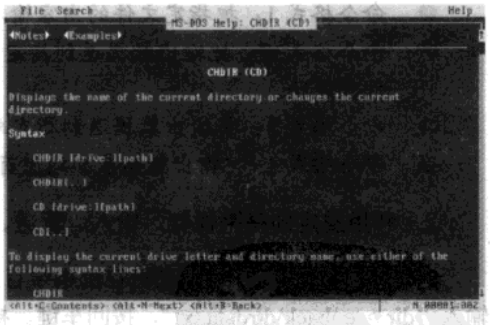


图 5-29

如果将光标移至“Notes”上，按回车键即可查询到 cd 命令的详细语法及功能的解释；如果将光标移至“Examples”上，按回车键即可查询到 cd 命令的语法的详细举例示范，如图 5-30 所示。

也可以按 Alt+S 键，打开“Find”（查找）对话框，利用“Find”来查找所需要了解的 DOS 命令。如需要了解“format”命令的详细信息，只需要在“Find What”框中输入“format”命令，如图 5-31 所示。

按回车键，即可查询到 format 命令的详细信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

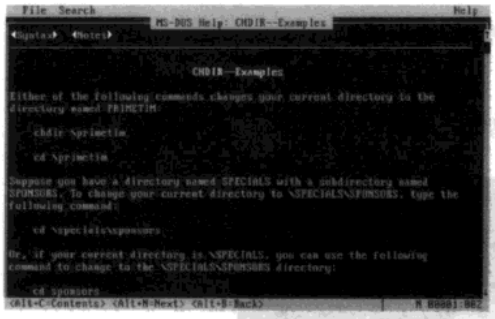


图 5-30

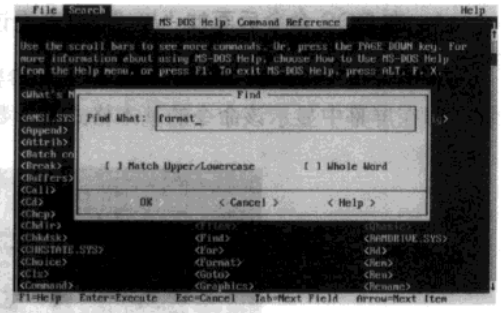


图 5-31

案例 41　在 DOS 下如何利用重定向符来保存、输入、发送、打印文件（<、>）

在 DOS 下重定向符的运用非常灵活，它们不但具有输出、输入的功能，还具有打印、发送的功能。DOS 中重定向符主要有 3 种，分别是“<”、“>”和“>>”，下面分别来看看它们各自的用法。

1. 认识重定向符命令格式

```
命令格式 1：<  [<盘符>][<路径>]<文件名>[.<扩展名>]
命令格式 2：>  [<盘符>][<路径>]<文件名>[.<扩展名>]
命令格式 3：>  <设备名>
命令格式 4：>>  [<盘符>][<路径>]<文件名>[.<扩展名>]
```

功能说明如下。

- 命令格式 1：把指定文件的内容输入到特定文件中。
- 命令格式 2：把输出数据送到指定名称的新文件中，如果已存在同名文件，则原文件被删除。
- 命令格式 3：将输出数据送到指定外部设备。
- 命令格式 4：把输出数据累加到原有文件之后，如果无此文件，则功能同命令格式 1。

2. 利用重定向符来保存、输入、发送、打印文件

若将屏蔽显示的目录信息保存到指定目录下的 dirdata.txt 数据文件中，可以在提示符后输入“dir > e:\back\dirdata.txt”，按回车键。接着在提示符后输入“type e:\back\dirdata.txt”，按回车键，即可看到将 C 盘根目录下的目录信息输入到 dirdata.txt 数据文件中，如图 5-32 所示。

若将 A 盘符下所有以 bat 为扩展名的文件的目录信息，累加输入到 dirdata.txt 数据文件中，可以在提示符后输入“dir a:*.bat >> e:\back\dirdata.txt”，按回车键。接着在提示符后输入“type e:\back\dirdata.txt”，按回车键，即可看到已经将 A 盘中所有以 bat 为扩展名的文件的目录信息累加输入到 dirdata.txt 数据文件中，如图 5-33 所示。

若用户已经在 DOS 下安装了打印机驱动程序，可以利用打印机直接将文件打印输出。如用户想把 dirdata.txt 文件利用打印机输出，只需要在提示符后输入“dir e:\back\dirdata.txt >prn”，按回车键，即可等待打印机进行打印输出。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

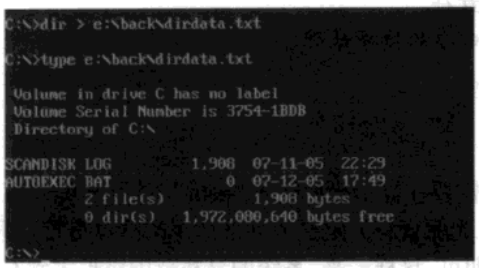


图 5-32

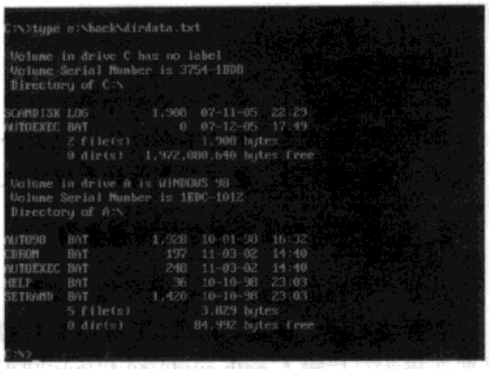


图 5-33

如果用户没有安装打印机，可以将屏幕作为标准输出设备。如使用 more 命令将 dirdata.txt 文件内容在屏幕输出，可以在提示符后输入“more < e:\back\dirdata.txt”，按回车键即可，如图 5-34 所示。

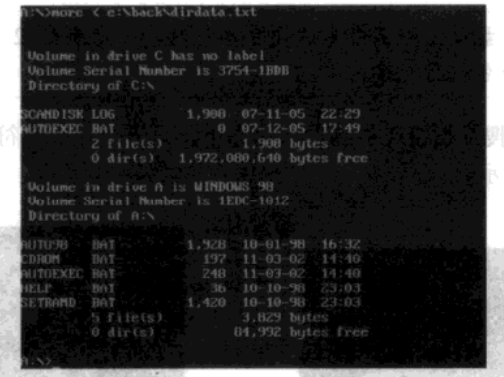


图 5-34

这个命令与输入“type e:\back\dirdata.txt | more”后按回车键的作用相同（关于“| more”的作用参考第 192 页“type”命令的说明）。

案例 42 如何在 DOS 下执行更多的内外部命令

在 DOS 中，如果当前提示符不是在启动盘符下，输入某一个外部命令却提示“Bad command or file name”（输入的命令无效）。但是在 DOS 启动盘符下此命令却是存在的，而且也可用。出现这种情况是因为想要执行的外部命令不在当前目录下，而在执行命令时也未指明路径，DOS 则认为命令出错。而 path 命令可以设定当一个希望执行的命令不在当前目录下时，DOS 自动搜寻的路径。

1. 认识 path 命令格式

```
命令格式 1：path
命令格式 2：path [<盘符>]<路径>; [<盘符>]<路径>……
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

命令格式 3：path;

功能说明如下。

- 命令格式 1：显示定义的外部命令搜寻盘符。
- 命令格式 2：定义多个盘符路径为外部命令的搜寻盘符。
- 命令格式 3：返回到最初的无定义状态。

2. 定义或还原外部命令的搜寻盘符

若要查看当前定义的外部命令搜寻盘符，只需要在提示符后输入“path”，按回车键即可。

若要将 C 盘、D 盘、E 盘、F 盘以及 G 盘（光驱盘符）定义为外部命令的搜寻盘符，只需要在提示符后输入 path c:\;d:\;e:\;f:\;g:\<回车>即可。这样一来，系统的寻找范围将扩大到 C、D、E、F、G 这 5 个盘符的根目录中，如图 5-35 所示。

但是有的用户在定义外部命令搜寻盘符时，将 A 盘也作为其中之一的搜寻盘符，即“path a:\;c:\;d:\;e:\;f:\;g:\”，按回车键。这样会带来麻烦，即 A 盘必须随时插有软盘；否则，将容易发生“磁盘未准备好”的错误提示。因此，不推荐使用这样的调用。

注意 在定义多个盘符为外部命令的搜寻盘符时，一定要在 2 个盘符之间用“;”隔开，否则命令执行无效。

若要将外部命令的搜寻盘符还原到默认状态下，只需要在提示符后输入“path;”，按回车键即可，如图 5-36 所示。

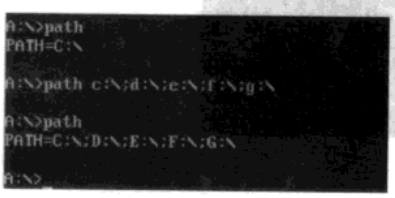


图 5-35

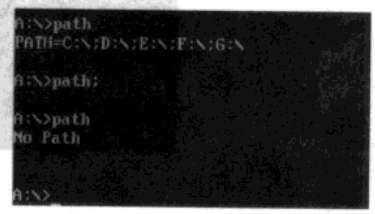


图 5-36

案例 43 在 DOS 下恢复误格式化分区中的文件

若在 DOS 下一不小心误格式化了某个分区，此时可以利用 unformat 命令进行恢复。但格式化后若做了其他数据的写入，则 unformat 命令就不能完整地救回数据了。除了可以恢复数据外，unformat 还可以对受损的系统扇区（包括 FAT、根目录、BOOT 扇区及硬盘分区表）进行抢救。

1. 认识 unformat 命令格式

命令格式：unformat〈盘符〉[/l][/u][/p][/test]

参数说明如下。

- /l：列出恢复后的子目录名称、文件名称、大致日期等信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- /u：不使用 MIRROR 映像文件的数据，直接根据磁盘现状进行 unformat。
- /p：将显示于屏幕的报告（包含/L 参数所产生的信息）同时也送到打印机。运行时屏幕会显示：“Print out will be sent to LPT1”。
- /test：只做模拟试验(test)不做真正的写入动作。使用此参数屏幕会显示：“Simulation only”。
- /psrtn：修复硬盘分区表。

小知识 若在盘符之后加上/p、/l、/test 其中之一，都相当于使用了/u 参数，unformat 会“假设”此时磁盘没有 MIRROR 映像文件。

2. 利用 unformat 命令来恢复误格式化分区中的文件

为了演示利用 unformat 命令来恢复格式化分区中的文件，这里以 F 盘为例。首先利用 format 对 F 盘进行格式化，如图 5-37 所示。

当格式化完毕后，在提示符后输入“unformat f:”，按回车键，即可弹出如图 5-38 所示的对话框。

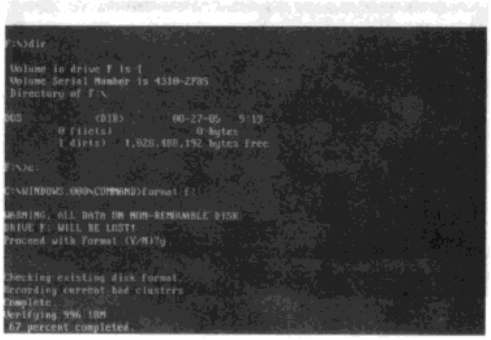


图 5-37

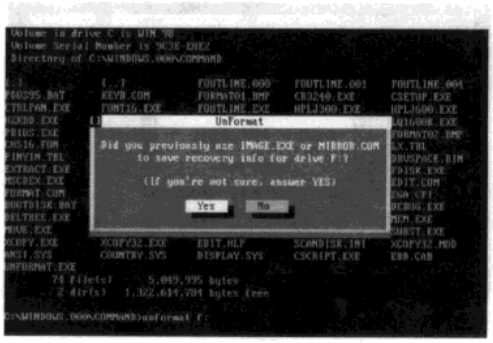


图 5-38

若要对数据进行恢复，这里直接按回车弹出如图 5-39 所示的对话框，再次询问用户是否撤消格式化且对数据进行恢复。同样直接按回车键，unformat 程序开始对 F 盘进行磁盘扫描，如图 5-40 所示。



图 5-39

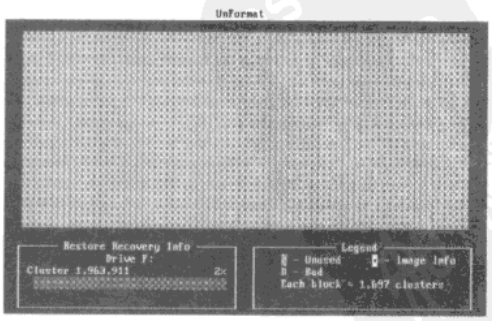


图 5-40

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

对 F 盘扫描完成后，弹出扫描报告，并询问用户是否继续执行下面的恢复操作，如图 5-41 所示。选中“Yes”按钮，按回车键将继续扫描并恢复数据，如图 5-42 所示。



图 5-41

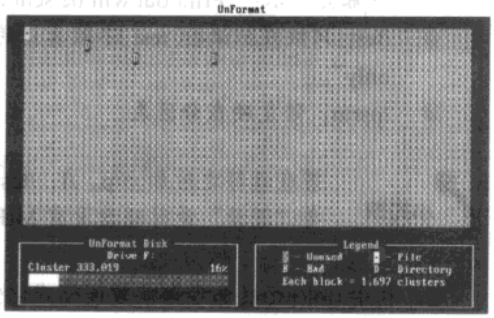


图 5-42

当误格式化分区中的数据恢复完毕后，弹出如图 5-43 所示的对话框。按回车键进入如图 5-44 所示的对话框中，提示数据已经恢复，可以退出 UnFormat。



图 5-43

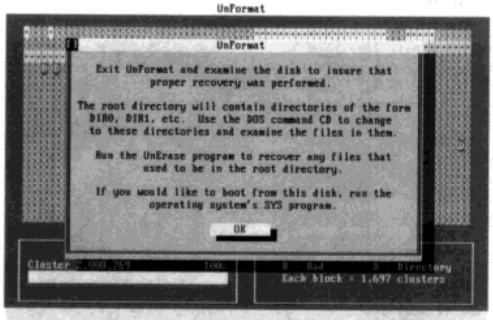


图 5-44

退出 UnFormat 后，在 DOS 下进入 F 盘，可以看到格式化之前的数据已经被恢复了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第6章 备份、恢复经典案例

当病毒攻击、人为损坏等因素，导致硬盘中重要的记录和数据丢失，甚至破坏了系统而无法启动时，读者会因无法找回丢失的数据而感到束手无策。为了防患于未然，做好硬盘记录、数据和系统备份是十分必要的。本章将介绍如何在 DOS 下备份、恢复硬盘主引导记录、注册表数据和操作系统。

案例 44 在 DOS 下备份、恢复主引导记录（MBR）

要在 DOS 下备份、恢复主引导记录，可以通过下面的方法来实现。

1. 备份主引导记录

下面介绍使用 debug 命令和三茗硬盘医生工具，在 DOS 下备份主引导记录的方法。

（1）利用 debug 命令备份主引导记录

先要将 debug 命令复制到 DOS 启动盘中，接着利用启动盘进入 DOS 系统中（本例以光盘启动盘为例），在提示符下运行 debug 命令，如图 6-1 所示。

首先，根据提示输入如图 6-2 所示的指令。

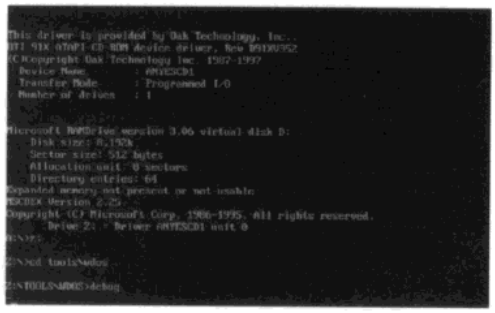


图 6-1

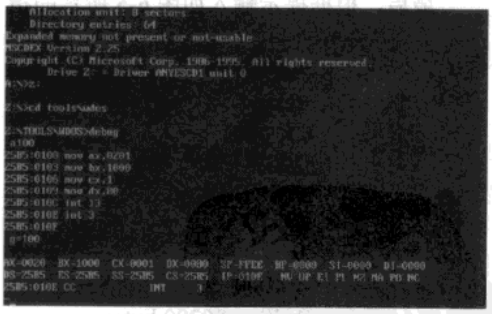


图 6-2

命令解析

```
Z:\TOOLS\WDOS\>debug          ；启动 debug 命令
-a100                         ；输入汇编程序
25B5:0100 mov ax,0201         ；读一个扇区
25B5:0103 mov bx,1000         ；缓存区地址=1000H
25B5:0106 mov cx,1            ；读 0 柱 1 扇区
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
25B5:0109 mov dx,80                    ；读 C 盘 0 头，驱动器号=80
25B5:010C int 13                       ；磁盘读写中断
25B5:010E int 3                        ；磁盘断点中断
25B5:010F                              ；结束输入
-g=100                                 ；执行程序
AX=0020 BX=1000 CX=0001 DX=0080 SP=FFEE BP=0000 SI=0000 DI=0000
DS=25B5 ES=25B5 SS=25B5 CS=25B5 IP=010E NV UP EI PL NZ NA PO NC
25B5:010E CC              INT     3    ；注意进位标志必须是 NC
```

接着，再根据提示输入如图 6-3、图 6-4 所示的指令。

接着，再根据提示输入如图 6-3、图 6-4 所示的指令。

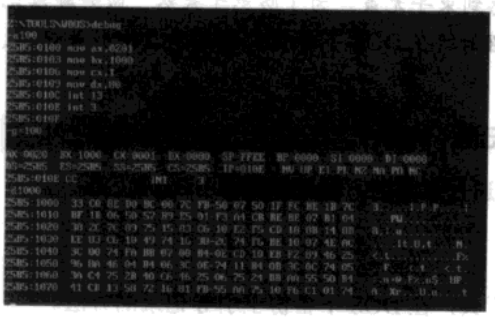


图 6-3

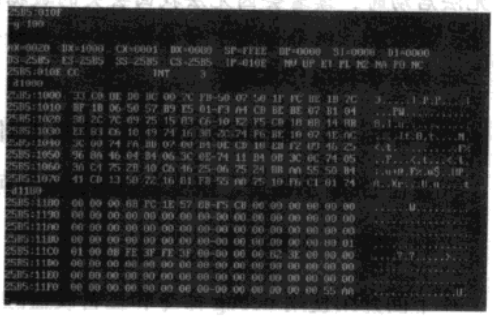


图 6-4

命令解析

```
-d1000                                 ；查看主引导扇区头部
-d1180                                 ；查看主引导扇区尾部
```

最后，根据提示输入如图 6-5 所示的指令。

命令解析

```
-nzdq.com                              ；指定文件名为 zdq.com
-rcx                                   ；指定写入长度为 200H 字节
CX 0001
:200
-rbx
BX 1000
:0
-w1000                                 ；写入
Writing 00200 bytes
-q                                     ；退出 debug
```

上面的指令执行完成后，主引导记录也就备份完成。

（2）利用三茗硬盘医生备份主引导记录

除了使用 debug 命令来备份主引导记录外，还有一些操作简单的硬盘维护、修复工具也可以用来备份主引导记录，如三茗硬盘医生、KV3000 等，这里以三茗硬盘医生为例介绍具体的备份操作。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

三茗硬盘医生只有 17KB 大小，可以从各大主流网站下载，如华军软件园、PChome 等。下载后，复制到 DOS 启动盘中，利用启动盘进入 DOS，运行 hdd21.com 或 hdd21.exe 即可进入“三茗硬盘医生”主界面，如图 6-6 所示。

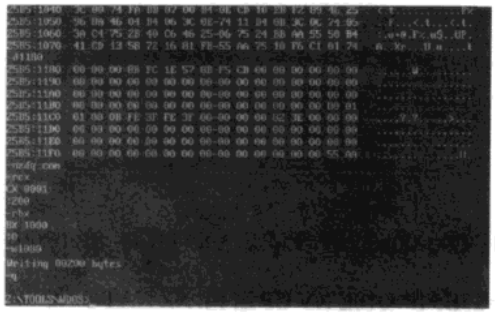


图 6-5

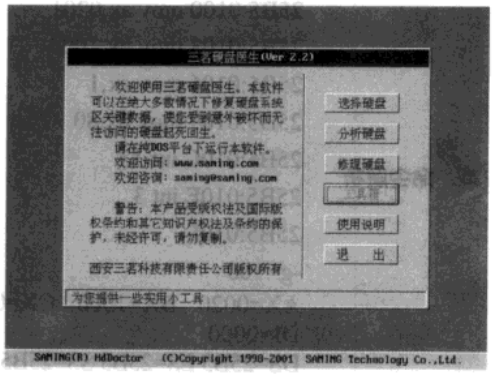


图 6-6

在主界面中选中“工具箱”，按回车键后进入图 6-7 所示的界面中。从该界面中选中“备份主引导扇区”按钮，按回车键即可将主引导扇区备份到该软件默认的保存位置，如图 6-8 所示。

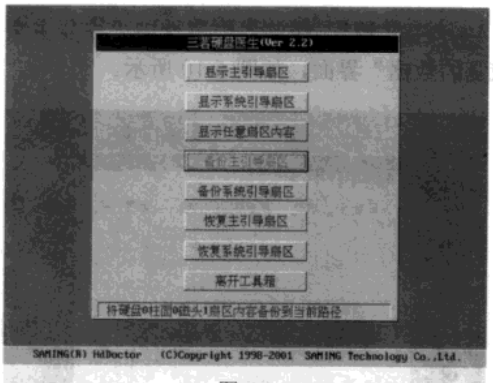


图 6-7

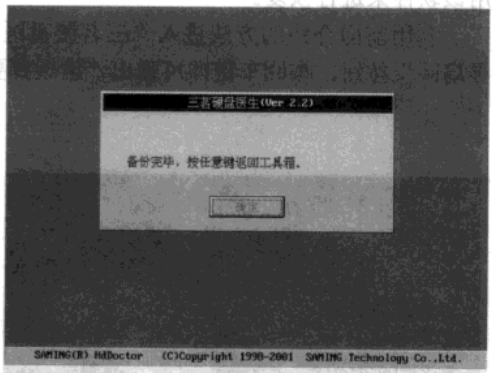


图 6-8

2. 恢复主引导记录

当主引导扇区被损坏，或发现病毒改写、覆盖了硬盘的主引导扇区，可以将上面备份的主引导记录回写到硬盘中，即恢复主引导记录。

（1）利用 debug 命令恢复主引导记录

若使用 debug 命令备份了主引导记录后，当主引导扇区损坏或感染了病毒，就可以利用 debug 命令恢复主引导记录。

利用启动盘进入 DOS 下，运行 debug 命令，接着根据提示输入如图 6-9 所示的指令。

当指令执行后，进位标志为 NC，即表示恢复成功。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

命令解析

```
Z:\TOOLS\WDOS\>debug          ；启动 debug 命令
-nzdq.com                     ；读备份的硬盘主引导记录
-a100                         ；将备份的主引导记录到 100H 处
25B5:0100 mov ax,0201         ；读恢复到的扇区位置
25B5:0103 mov bx,1000         ；缓存区地址=1000H
25B5:0106 mov cx,1            ；读 0 柱 1 扇区
25B5:0109 mov dx,80           ；读 C 盘 0 头，驱动器号=80
25B5:010C int 13              ；读写中断
25B5:010E int 3               ；断点中断
25B5:010F                     ；结束输入
-g=100                        ；执行程序
AX=0020 BX=1000 CX=0001 DX=0080 SP=FFEE BP=0000 SI=0000
DI=0000
DS=25B5 ES=25B5 SS=25B5 CS=25B5 IP=010E NV UP EI PL NZ NA PO NC
25B5:010E CC      INT     3   ；回写，注意进位标志为 NC 表示成功；
否则失败。
```

（2）利用三茗硬盘医生恢复主引导记录

上面已经使用三茗硬盘医生对主引导记录进行了备份，如果主引导记录损坏，也可以利用该软件来进行恢复。

利用前面介绍的方法进入“三茗硬盘医生”→“工具箱”，在该界面中选中“恢复主引导扇区”按钮，按回车键即可弹出“请选择要恢复的数据”界面，如图 6-10 所示。



图 6-9

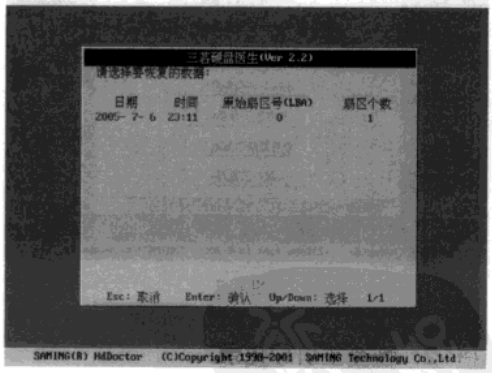


图 6-10

如果经常备份主引导记录，它会将每次备份的信息单独作为一条记录保存起来，当恢复主引导记录时会在图 6-9 所示的界面中显示每次备份的时间。用户进入该界面后，只要选择某一条正确的备份记录，按回车键，即可将备份的主引导记录恢复到硬盘中。

案例 45　在 DOS 下备份、恢复分区表记录

在 DOS 下备份、恢复分区表记录，可以使用 debug 命令，也可以使用 DOS 下的小工具，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如 Disk Genius、KV3000 等，这里以 Disk Genius 工具为例进行说明。

1. 利用 Disk Genius 工具备份分区表记录

首先进入“Disk Genius”主界面，接着单击“工具”→“备份分区表”命令，如图 6-11 所示。接着弹出“备份到文件”对话框，在“请输入文件名”框中输入分区表的备份路径，默认情况下是备份到软盘中，如图 6-12 所示。

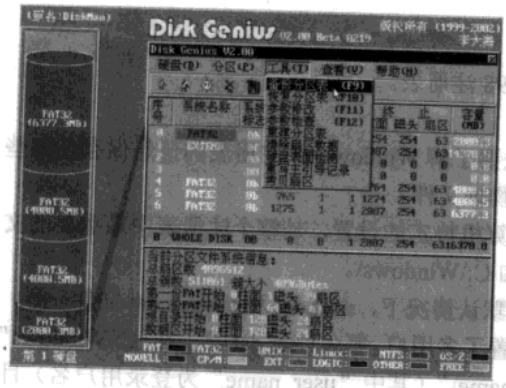


图 6-11

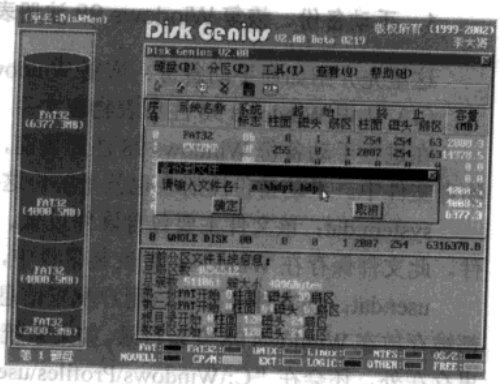


图 6-12

输入好具体的备份路径后，单击“确定”按钮即可。

2. 利用 Disk Genius 工具恢复分区表记录

如果用户是利用 Disk Genius 工具来备份硬盘分区表记录，当主分区表损坏后，就可以利用 Disk Genius 工具来恢复它。

单击“工具”→“恢复分区表”命令，弹出“从备份恢复分区表”对话框。在“请输入文件名”框中输入分区表备份的具体路径，默认情况下是从软盘来读取备份文件恢复分区表记录，如图 6-13 所示。



图 6-13

输入正确的备份文件路径后，单击“确定”按钮恢复分区表，最后重新启动系统即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

案例 46　在 DOS 下手动备份、恢复注册表

注册表是操作系统的核心，因为几乎所有的系统配置信息都保存在注册表中。一旦注册表损坏，系统将无法启动或会运行出错，所以有计划地备份注册表是十分必要的。

虽然逻辑上注册表是一个数据库，但为了易于管理和使用，系统在物理上把它分为两个文件：user.dat（用户设置）和 system.dat（系统设置）。因此可以用复制法来备份这些文件。

1. 手动备份、恢复 Windows 98 注册表

这里先介绍如何手动备份、恢复 Windows 98 注册表。

（1）认识 Windows 98 注册表物理文件

在进行手动备份 Windows 98 注册表前，先要了解 Windows 98 注册表的信息保存在哪些物理文件中。手动备份注册表也就是备份这些物理文件。

system.dat：该文件主要包含硬件设置、计算机特定的设置，是整个注册表中最重要的文件。此文件保存在 Windows 98 安装目录中，如 C:\Windows\。

user.dat：该文件主要包含用户配置信息。默认情况下，user.dat 和 system.dat 文件一样，都被存放在 Windows 98 安装目录。如果系统配置了多用户，那么 User.dat 除了在“C:\Windows”里存在外，还会在“C:\Windows\Profiles\user_name\”（其中“user_name”为登录用户名）目录中存在。

system.ini、win.ini：虽然这两个文件在 Windows 98 中的作用已经很小了，但一些老的 16 位应用程序仍然会用到它们，而注册表也将从这两个文件中读取 16 位应用程序的兼容信息。所以完整的注册表备份中应该包含这两个文件。这两个文件同样也保存在 Windows 98 的安装目录中。

作为一个完整可靠的注册表备份，以上文件都是必须的。

（2）手动备份恢复 Windows 98 注册表

假设已经在 Windows 下将上述注册表文件备份在 D:\regbak 文件夹下，并且去除了它们的隐藏属性、只读属性，那么在 DOS 下恢复注册表的操作步骤如下。

首先，利用启动盘启动系统或在 Windows 98 系统启动时按 F8 键，选择“Command prompt only”进入 DOS。

接着，利用 attrib 命令去除 user.dat、system.dat 文件的只读属性和隐藏属性。

然后进入 D:\regbak 目录，依次运行如下命令，如图 6-14 所示。

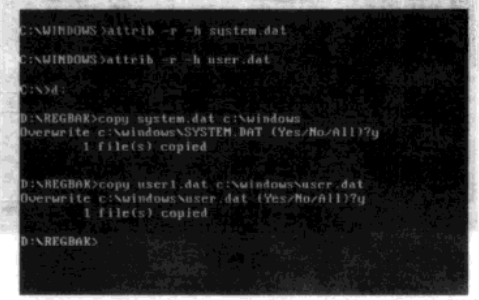


图 6-14

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- copy D:\regbak\system.dat C:\Windows
- copy D:\regbak\user1.dat C:\Windows\user.dat
- copy D:\regbak\user2.dat C:\Windows\Profiles\user_name\user.dat
- copy D:\regbak\win.ini C:\Windows
- copy D:\regbak\system.ini C:\Windows

文件复制完成后，重启启动系统即可。

2．手工备份、恢复 Windows 2000/XP/2003 注册表

在 Windows 2000/XP/2003 下对注册表进行备份与恢复要比 Windows 98 下复杂得多，原因之一就是，Windows 2000/XP/2003 的注册表物理文件再也不像在 Windows 98 中的那样只有几个了，取而代之的是一系列的注册表文件。下面来全面了解这些物理文件。这里以 Windows XP 为例，假定系统安装在 C 盘，系统目录为 C:\Windows（如果是 Windows 2000/2003，系统目录为 C:\WINNT）。

（1）认识 Windows 2000/XP/2003 注册表物理文件

Windows 2000/XP/2003 注册表的物理文件集中在%SystemRoot%\System32\Config 目录下，这里有 20 个左右的文件，有不带后缀的，有这里的“%SystemRoot%”表示系统安装目录，下同。带.log、.evt 后缀的。

.log 文件：.log 文件（Default.Log，Sam.Log，Security.Log，Software.Log，System.Log，以及在另一位置的 ntuser.dat.Log）只有在注册表进行某种更新的过程中，遇到计算机意外地关机时才有用。一般情况下，这些文件不是最需要备份的。

.sav 和修复文件：.sav 文件（default.sav、sam.sav、security.sav、software.sav 和 system.sav）是计算机安装 Windows 2000/XP/2003 时，注册表处于初始状态时的版本。它们不是注册表文件的备份副本（这有些类似 Windows 98 的 system.1st 文件）。


小知识

确切地说，.sav 是在安装程序的文本模式结束后，但在安装程序的图形模式结束前初级注册表的快照。.sav 文件存在的原因是，万一遇到安装程序的图形部分出故障时，安装不需要从头开始。

.alt 文件：这类文件只有一份，即 system.alt，它是 system 文件的镜像。如果计算机正好在修改注册表的那一刻非正常关闭（比如断电），用 system.alt 替换 system 就能解决问题。

无扩展名文件：真正最重要的注册表文件，就是保存在%SystemRoot%\System32\Config 文件夹下的那些不带扩展名的文件：Dfault、Sam、Security、Software、System、USERDIFF（Windows XP 多用户机制所特有）。任何注册表备份方案都必须把这些文件包括进去。

用户指定文件：不是所有的注册表文件都存放在%SystemRoot%\System32\Config 中。与用户有关的设置（存放在名为 ntuser.dat 的文件中）可存放在不同地点，一般这些文件存放在 C:\Documents And Settings\<Username>文件夹或 C:\Winnt\Profiles\<Username>文件夹下（其中的<Username>为当前计算机中的注册用户名）。在 Windows 2000/XP 中，有账户的每一个用户都设立了一个单独的 ntuser.dat 文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

提示 如果想知道 Windows 2000/XP 上有多少 ntuser.dat，使用开始菜单的搜索功能搜索 C 盘（安装 Windows 2000/XP 的盘符），并在搜索关键字中输入“ntuser.dat”，这样就能找到系统中所有用户的 ntuser.dat 文件。

（2）手动备份、恢复 Windows 2000/XP/2003 注册表

备份、恢复 Windows 2000/XP/2003 注册表，系统盘文件系统不同，备份和恢复方法也不相同。

① FAT32 文件系统

系统盘为 FAT32 格式的好处是，用户可以通过一张启动盘启动到 DOS 下，然后把注册表文件从备份位置覆盖到系统位置。

仍然假设备份文件保存在 D:\regbak 位置，操作系统为 Windows XP；首先用启动盘启动到 DOS 下，进入 D:\regbak 目录，依次执行如下命令。

```
copy System C:\Windows\System32\config（如图 6-15 所示）
copy Software C:\Windows\System32\config
copy Sam C:\Windows\System32\config
copy Default C:\Windows\System32\config
copy Security C:\Windows\System32\config
```

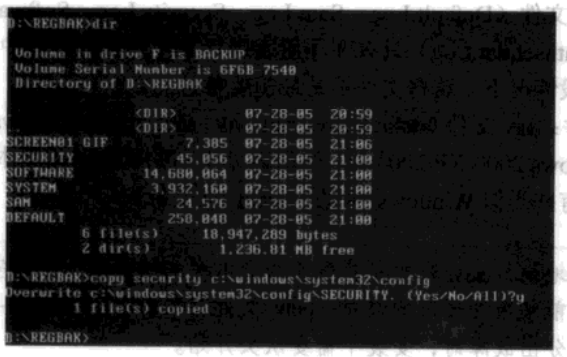


图 6-15

如果备份了其他注册表文件，继续执行上述操作，把文件还原到系统原来的位置。

② NTFS 文件系统

如果系统盘为 NTFS 格式，普通的启动盘无法把系统启动到 DOS 下（后面章节讲到的超级启动盘除外），这时就需要用到故障恢复控制台（一个类似 DOS 的环境）。通过故障恢复控制台，用户可以像在 DOS 中一样从备份位置把注册表文件覆盖到系统位置。

需要注意的是，默认情况下，故障恢复控制台不允许对系统盘之外的分区下的文件夹进行操作，所以建议将备份文件保存在系统分区。

假设备份文件保存在“C:\winnt\regbak”下面，系统为 Windows 2000。首先从 Windows 2000 安装光盘引导进入故障恢复控制台（进入“恢复控制台”的方法请参阅第 7 章的第 1 个案例），或从安装的故障恢复控制台启动菜单项进入故障恢复控制台，然后依次执行如下命令。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
copy system c:\winnt\system\config（如图 6-16 所示）
copy sam c:\winnt\system\config
copy software c:\winnt\system\config
copy security c:\winnt\system\config
copy default c:\winnt\system\config
```

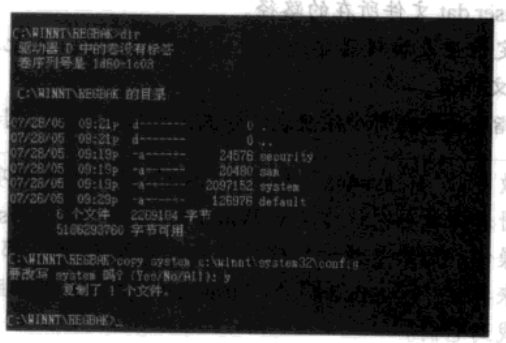


图 6-16

如果备份了其他注册表文件，继续执行上述操作，把文件还原到原来的位置。

③ 多操作系统

如果安装了多操作系统，可以在其他操作系统中从备份位置恢复注册表，如同直接在本操作系统中操作一样。

案例 47 在 DOS 下利用注册表编辑器备份、恢复注册表

其实，Regedit.exe（注册表编辑器程序）不仅能在 Windows 环境中运行，在 DOS 下也能运行。虽然在 DOS 下运行的功能没有在 Windows 平台中那样强大，但是备份注册表信息还是比较快捷、方便的。

注意 注册表文件一般放置在 C:\Windows 中。Windows 2000/2003 放置在“C:\WINNT”中，Windows XP 放置在“C:\Windows”中。

首先，利用启动盘进入 DOS，接着进入“C:\Windows”下，在命令提示符下运行“regedit.exe”，按回车键，出现如图 6-17 所示的信息。

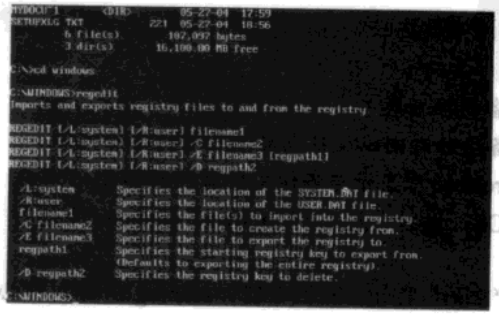


图 6-17

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

图中显示了 Regedit 的所有参数。Regedit 具体的命令格式如下。

```
命令格式：regedit /l:system /r:user /e filename.reg regpath
```

参数说明如下。

- /l：system 指定 system.dat 文件所在的路径。
- /r：user 指定 user.dat 文件所在的路径。
- /e：此参数指定注册表编辑器要进行导出注册表操作，在此参数后面空一格，输入导出注册表的文件名。
- regpath：用来指定要导出哪个注册表的分支，如果不指定，则将导出全部注册表分支。

注意 在这些参数中，“/l：system”和“/r：user”参数是可选项。如果不使用这两个参数，注册表编辑器则认为是对 Windows 目录下的“system.dat”和“user.dat”文件进行操作。如果是通过从软盘启动并进入 DOS，那么就必须使用“/l”和“/r”参数来指定“system.dat”和“user.dat”文件的具体路径，否则注册表编辑器将无法找到它们。

这里要备份注册表信息，就可以使用以下命令。

```
regedit /l:C:\windows\/r:F:\ /e: regedit.reg
```

该命令的意思是把整个注册表备份到 F:\下，其备份文件名为“regedit.reg”。

案例 48　在 DOS 下利用注册表检查器备份、恢复注册表

除了按照上面的方法在 DOS 下利用注册表编辑器来备份外，还可以在 DOS 下利用注册表检查器来备份，具体操作如下。

注意 在 DOS 方式下使用的 scanreg.exe 程序与在 Windows 视窗界面中使用的 scanregw.exe 程序有着不同的功能和作用，这里大家不要混淆了（scanreg 命令位于“C:\Windows\”目录下）。

1．利用注册表检查器备份注册表

首先，来了解一下注册表检查器的命令格式。

```
命令格式：scanreg [参数]
```

参数说明如下。

- /backup：立即备份注册表。
- /restore：按照备份的时间以及日期显示所有的备份文件。
- /comment：在/restore 中显示与备份文件有关的部分。

利用启动盘进入 DOS，然后进入 C:\Windows\Command\下运行 scanreg，回车，进入图 6-18 所示的界面中。

在图 6-18 中选中“Start”按钮，按回车键，scanreg 开始对核心系统文件进行检测，当一切正常时，将进入图 6-19 所示的界面中。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

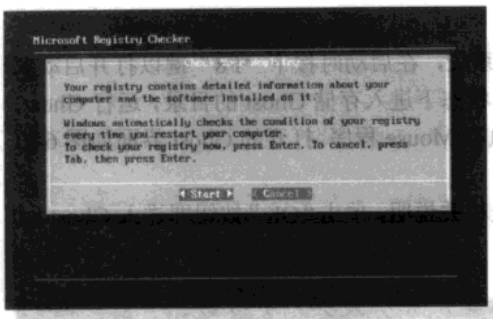


图 6-18

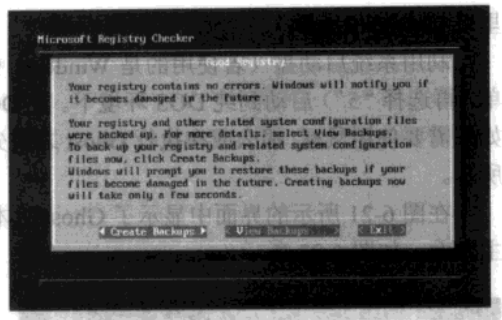


图 6-19

在图 6-19 中选中“Create Backups”按钮，按回车键即可备份注册表信息。scanreg 不提供备份路径，而是以默认的方式将注册表备份路径放在 C:\Windows\Sysbckup 中。备份完成后，选中“Exit”按钮，按回车键退出 scanreg。

2. 利用注册表检查器恢复注册表

如果利用 Scanreg 恢复注册表信息，可在图 6-19 所示的界面中选中“View Backups”按钮，按回车键，Scanreg 将显示 C:\Windows\Sysbckup 中的注册表备份文件，如图 6-20 所示。

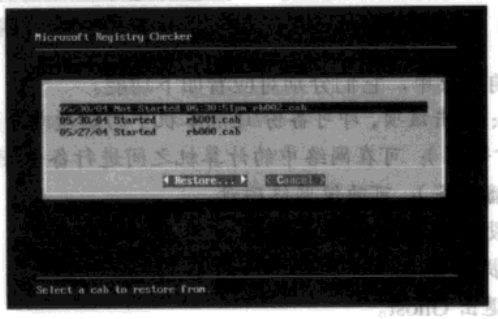


图 6-20

选择其中的一个 cab 包后，选中“Restore”按钮，按回车键进行恢复，完成后选中“OK”按钮，按回车键重新启动计算机，损坏的注册表就恢复正常了。

案例 49 在 DOS 下利用 Ghost 备份、恢复系统

Ghost 是“General Hardware Oriented Software Transfer”的缩写，即“面向通用型硬件传送软件”，它可将整个硬盘中的数据完全相同地复制到其他硬盘中，因此又称为硬盘“克隆”工具。同时还具有硬盘分区、硬盘备份、系统克隆、网络克隆、升级系统等功能。目前常见的 Ghost 版本有 Ghost 6.0、Ghost 7.0、Ghost 8.0 和 Ghost 9.0（这个版本可以在 Windows 系统下直接运行使用）。

1. 利用 Ghost 备份系统

无论使用哪个版本的 Ghost，在 DOS 下对系统进行备份、恢复的操作过程都是相同的（这

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

里以 Ghost 8.0 为例）。

利用系统启动盘（若使用的是 Windows 98 系统，在启动时按下“F8”键以打开启动菜单，再选择“5”）启动到纯 DOS 环境下。在 DOS 状态下进入存储 Ghost 的目录，运行 Ghost。如果需要使用鼠标，那么应在执行 Ghost 之前先执行 Mouse 程序。打开的 Ghost 界面如图 6-21 所示。

在图 6-21 所示的界面中显示了 Ghost 版本及相关说明，单击“OK”按钮即进入 Ghost 8.0 主界面，如图 6-22 所示。

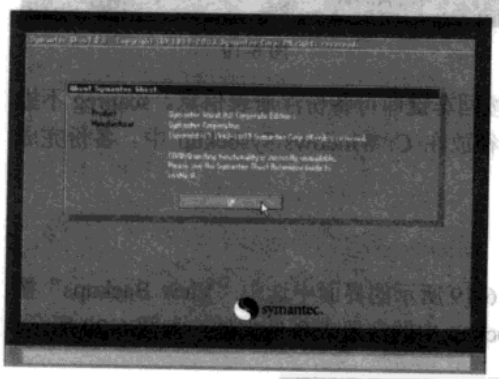


图 6-21

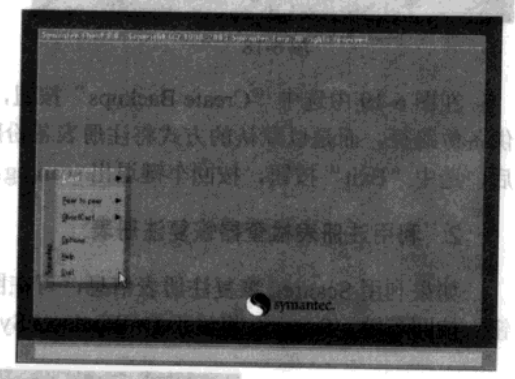


图 6-22

这里大致介绍左下角的菜单，它们分别对应着如下功能。

- Local（本地的）：单击该项，即可备份/还原本机中的磁盘或分区，是应用最多的一项。
- Peer to peer（对等的）：可在网络中的计算机之间进行备份/还原操作。
- GhostCast（多播服务）：可映像网络磁盘。
- Options（选项设置）：设置相关参数。
- Help（帮助）：提供帮助。
- Quit（退出）：退出 Ghost。

下面来详细介绍如何利用 Ghost 8.0 备份操作系统。在主界面中单击“Local”→“Partition”→“To Image”命令，如图 6-23 所示。在弹出的磁盘选择界面中，如果有多块硬盘要注意正确选择，选择完成后单击“OK”按钮确定。

接着进入要建立映像文件的磁盘分区，即选择系统所在的磁盘分区。由于备份的是 Windows 系统，所以选择“Primary”分区，如图 6-24 所示。

系统磁盘分区选中后，单击“OK”按钮确定，进入存储系统备份的路径下。注意，存储路径要选择系统分区之外的任意磁盘，并确保该磁盘有足够大的可用空间以保存系统备份的映像文件。在此选择 F 盘，并输入映像文件名“winxpback”，如图 6-25 所示。

设置完成后，单击“Save”按钮保存。接下来程序会询问是否压缩备份数据，并给出“No”按钮表示不压缩，“Fast”按钮表示压缩比例小而执行备份速度较快，“High”按钮就是压缩比例高但执行备份速度相当慢，如图 6-26 所示。

这里单击“High”按钮，在接下来的界面中单击“Yes”按钮，即可开始对系统进行备份操作，备份完成后单击“Continue”按钮即可，如图 6-27 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

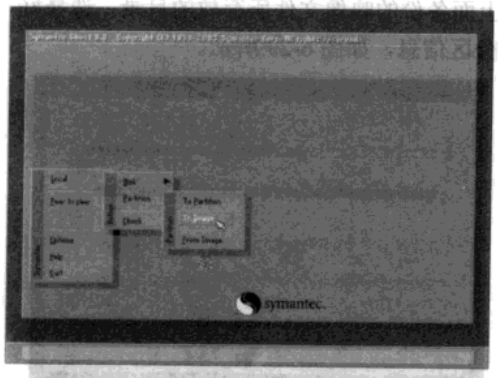


图 6-23

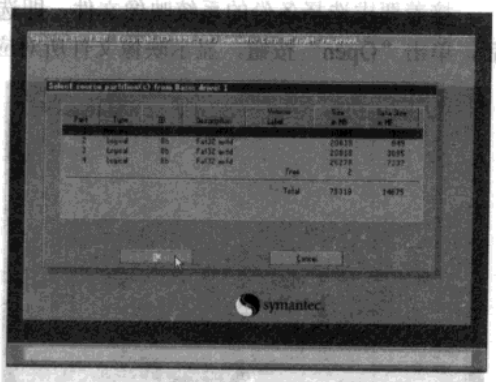


图 6-24

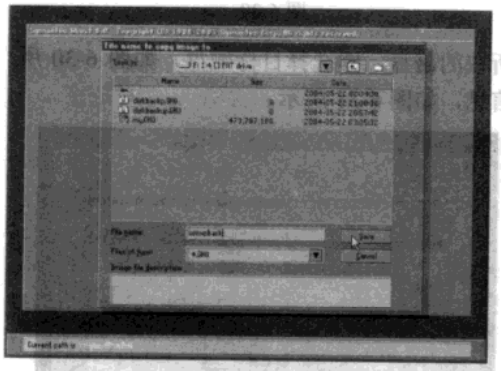


图 6-25

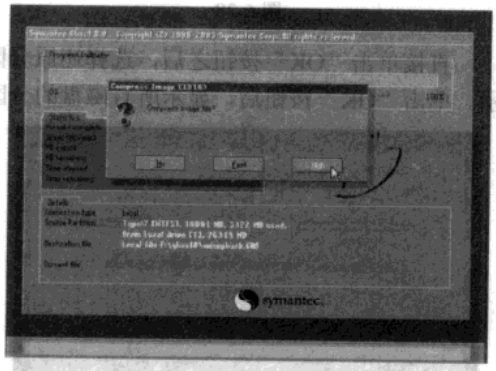


图 6-26

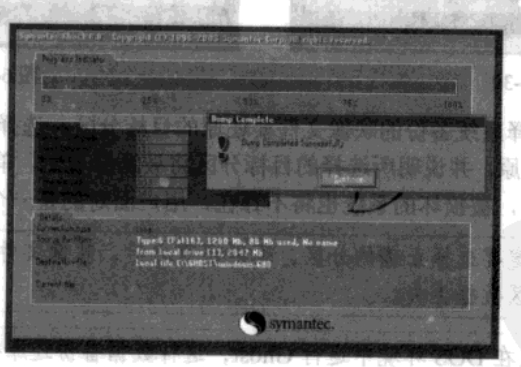


图 6-27

2. 利用 Ghost 恢复系统

当操作系统被损坏时，可以利用 Ghost 对系统进行恢复，也就是利用备份的映像文件来还原系统。进入 DOS 后，运行 Ghost，在主界面中单击“Local”→“Partition”→“From Image”命令，如图 6-28 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

接着要求选择备份的系统映像文件，即选择上面备份的映像文件所存放的目录。选择好后，单击“Open”按钮，显示映像文件所对应的分区信息，如图 6-29 所示。

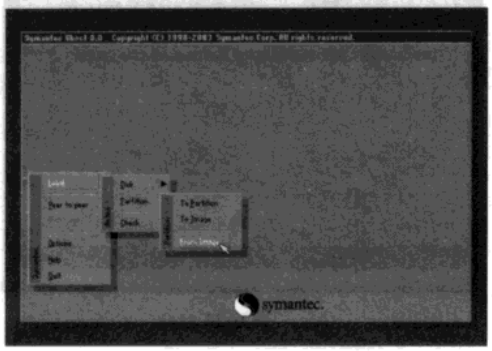


图 6-28

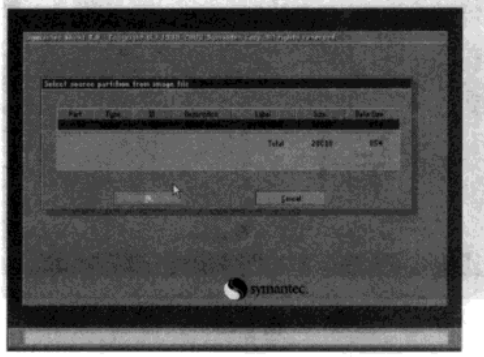


图 6-29

直接单击“OK”按钮之后，选择还原分区所在的磁盘，即选择目标磁盘，如图 6-30 所示。单击“OK”按钮后，显示所有磁盘的分区信息，如图 6-31 所示。

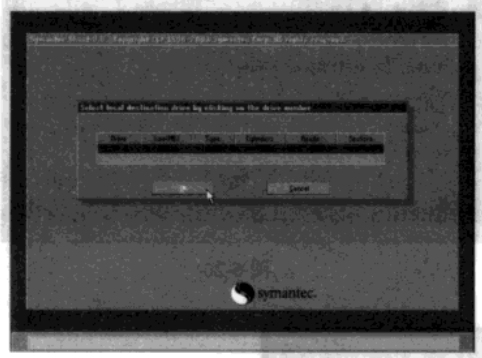


图 6-30

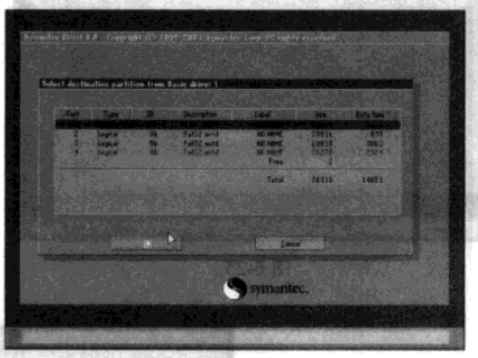


图 6-31

在图 6-31 中，选择系统备份的映像文件要还原的目标分区。选择完成后，单击“OK”按钮，提示是否执行还原，并说明所选择的目标分区将被还原覆盖。单击“Yes”按钮还原操作系统。当还原成功后，被损坏的系统也将不存在，用户面对的是一个完好的操作系统。

注意 此时，一定要选择正确的分区，否则还原之后，映像文件会覆盖误选的分区，导致该分区数据丢失。

小知识

① 建议在 DOS 环境中运行 Ghost，这样数据备份还原操作成功率高。

② 在备份磁盘或磁盘分区时，要先对磁盘或磁盘分区进行整理，如删除无用的数据资料、临时文件，执行磁盘碎片整理等，以便缩小将要建立的映像文件，从而让执行更快速，而且节省磁盘空间。

③ 在备份时，单个的备份文件大小一般不要超过 2GB。

④ 为了更安全地备份磁盘数据资料，可将建立的磁盘或分区映像文件保存在其他位置，如保存在另外的磁盘，或刻录到光盘等。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

案例 50 在 DOS 下利用 Ghost 备份、恢复分区映像

所谓备份分区映像，即将某一硬盘分区压缩为一个映像文件，并将映像文件存储在该分区之外的地方，如存储在该硬盘的其他分区，或存储在另外一块硬盘中，或刻录到光盘中等，即建立硬盘分区备份。

在利用 Ghost 备份分区映像操作之前，用户应确定将要建立备份的分区及分区映像文件的保存位置，如现需要备份 D 盘的数据资料，并将分区映像文件保存到 F 盘中。当 D 盘的数据受损后，可以从 F 盘读取映像文件以恢复 D 盘的数据资料。

1. 利用 Ghost 备份分区映像

进入 Ghost 主界面后，单击“Local”→“Partition”→“To Image”命令，如图 6-32 所示。接着打开选择磁盘界面，如果有多块硬盘要注意正确选择，选择完成后单击“OK”按钮确定。此时会显示磁盘所有的分区，如图 6-33 所示。

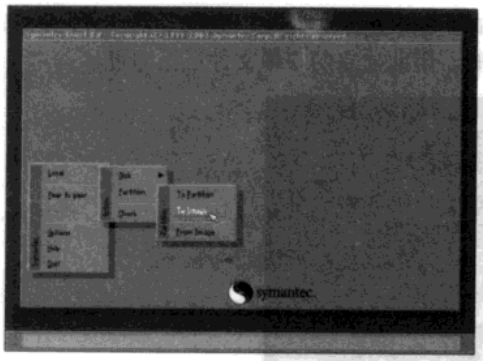


图 6-32

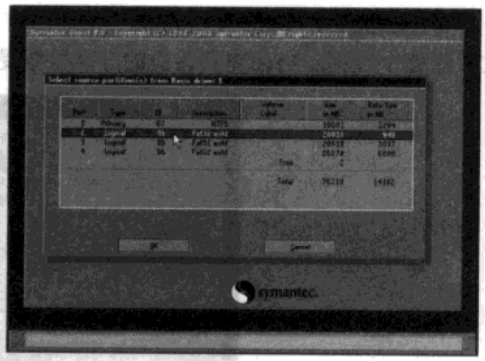


图 6-33

如果备份的是 D 分区，则选择第二项，单击“OK”按钮确定。接着进入保存映像文件界面，这里将备份的映像文件保存到 F 分区中，即在“Look in”中选中 F 分区，如图 6-34 所示，在“File Name”中输入映像文件名，如 mybackup。

设置完成后，单击“Save”按钮保存，接下来程序会询问是否压缩备份数据，如图 6-35 所示。

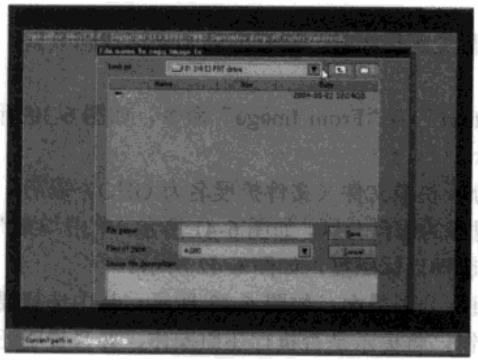


图 6-34

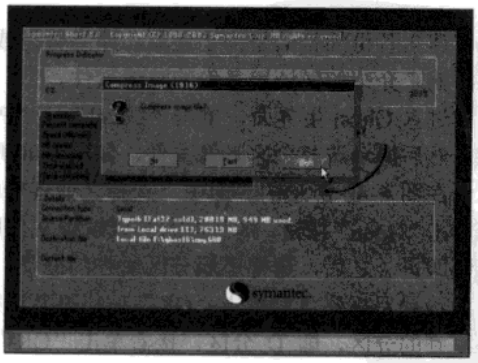


图 6-35

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这里单击“High”按钮，提示是否执行操作，如图 6-36 所示。单击“Yes”按钮即开始建立分区映像文件，如图 6-37 所示。

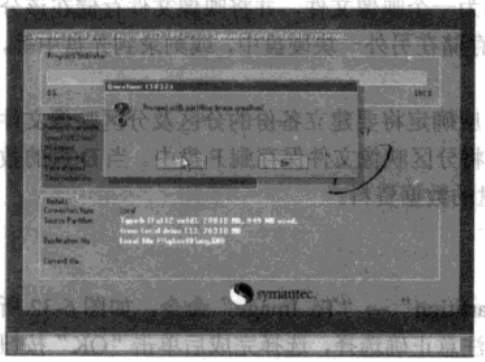


图 6-36



图 6-37

备份完成后，单击“Continue”按钮即可，如图 6-38 所示。至此，完成了建立分区映像文件的整个过程。当已建立备份的分区数据受损时，用此建立的映像文件还原即可。

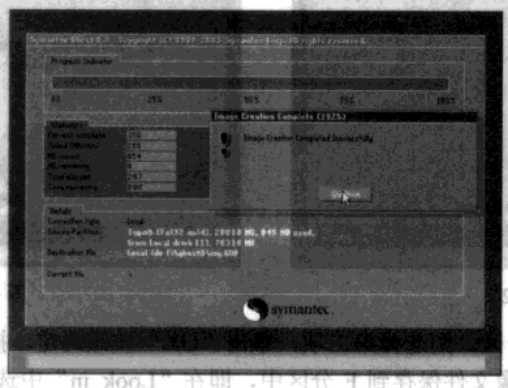


图 6-38

2. 利用 Ghost 恢复分区映像

建立备份的目的是为了还原，即当数据或硬盘受到损坏时，能够准确无误地找回数据。下面就来介绍如何还原备份的映像文件。

进入 Ghost 主界面，单击“Local”→“Partition”→“From Image”命令，如图 6-39 所示。然后提示选择分区映像文件，如图 6-40 所示。

在图 6-40 所示的界面中，选择之前备份的分区映像文件（文件扩展名为 GHO）以后，再单击“Open”按钮，接着提示分区映像文件所对应的磁盘分区，如图 6-41 所示，单击“OK”按钮即可。之后，选择还原分区所在的磁盘，即选择目标磁盘，如图 6-42 所示。

选择目标磁盘后单击“OK”按钮打开选择目标分区界面，如图 6-43 所示。从中选择要还原到的分区，即 D 分区。接着单击“OK”按钮，将提示是否执行还原操作，并且说明还原以后目标分区的数据资料将被覆盖，如图 6-44 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

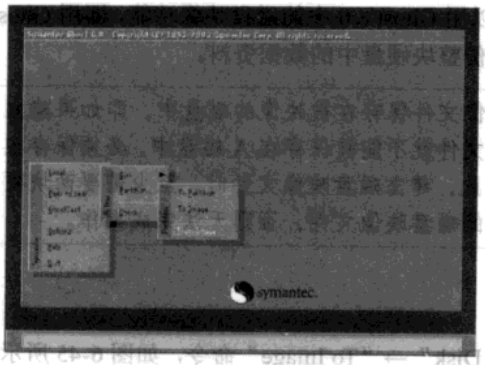


图 6-39

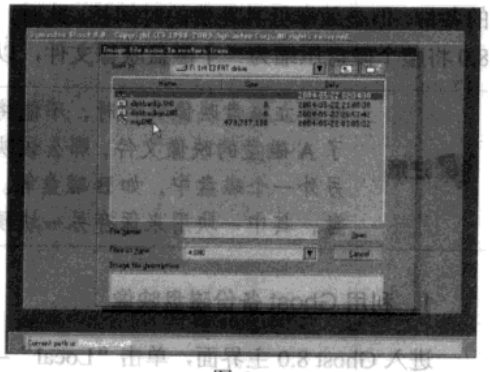


图 6-40

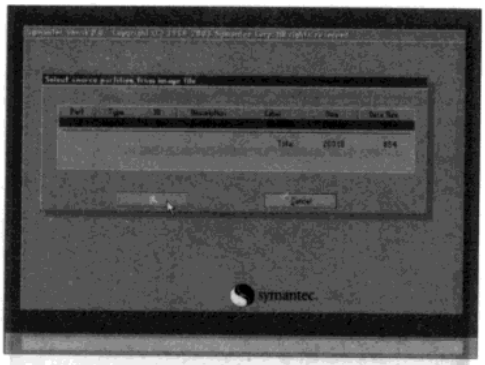


图 6-41

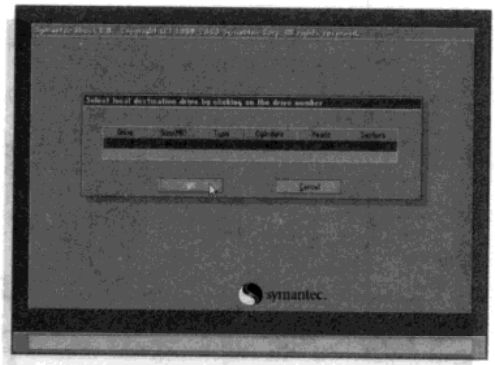


图 6-42

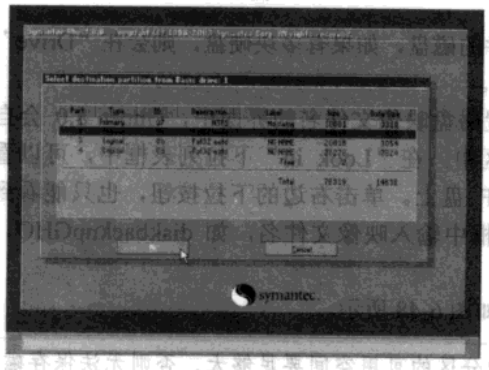


图 6-43

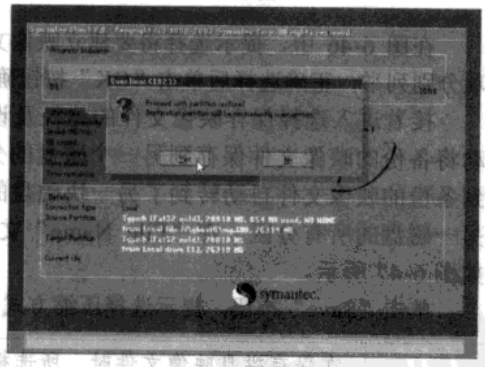


图 6-44

单击“Yes”按钮，即开始执行还原分区操作。完成后，之前备份的分区映像文件成功被还原，被还原的磁盘分区就又回到了最初备份时的状态，当时的数据资料又找回来了。

案例 51 在 DOS 下利用 Ghost 建立、恢复磁盘映像

上一案例是将硬盘的某个分区存储如一个映像文件，从而建立分区备份。但需要备份整个硬盘的数据资料时，是不是逐一备份硬盘中的所有分区呢？这么做当然可以完成整个硬盘

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

的备份，但是效率低且花费的时间长。此时，可以用 Ghost 8.0 中的磁盘映像功能，即用 Ghost 8.0 将整个硬盘压缩为一个磁盘映像文件，以备份整块硬盘中的数据资料。

注意 在建立磁盘映像文件时，不能将映像文件保存在被映像的磁盘中，即如果建立了 A 磁盘的映像文件，那么该映像文件就不能被保存在 A 磁盘中，必须保存在另外一个磁盘中，如 B 磁盘等。因此，建立磁盘映像文件时，至少需要两块硬盘，其中一块用来保存另一块硬盘的磁盘映像文件，否则无法完成操作。

1. 利用 Ghost 备份磁盘映像

进入 Ghost 8.0 主界面，单击“Local”→“Disk”→“To Image”命令，如图 6-45 所示。之后将看到磁盘选择界面，如图 6-46 所示。

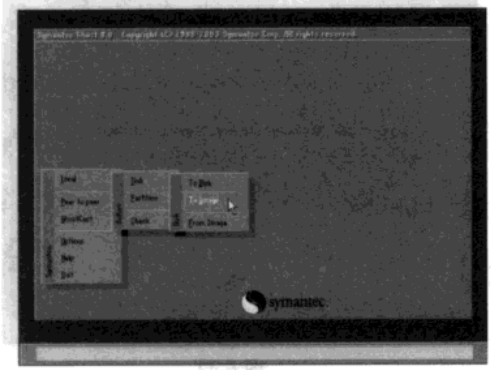


图 6-45

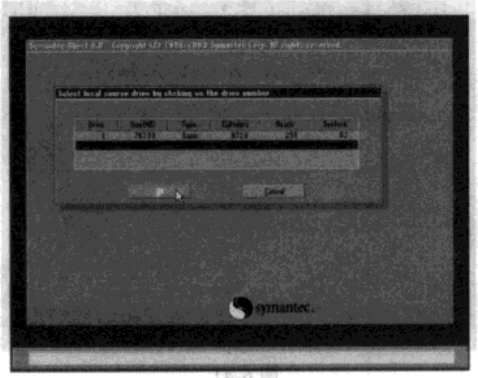


图 6-46

在图 6-46 中，提示选择将要建立映像文件的磁盘，如果有多块硬盘，则会在“Drive”项分别列举，正确选择后单击“OK”按钮确定。

接着进入选择保存映像文件的路径及设置磁盘映像文件名的界面中，Ghost 8.0 会自动将备份的映像文件保存到另一个磁盘的分区中。在“Look in”下拉列表框中，可以看到备份的映像文件自动转到了另一块磁盘的 F 盘上。单击右边的下拉按钮，也只能看到另一磁盘的所有分区。在“File Name”文本框中输入映像文件名，如 diskbackupGHO，如图 6-47 所示。

单击“Save”按钮，提示选择压缩方式，如图 6-48 所示。

注意 在保存磁盘映像文件时，所选择的分区的可用空间要足够大，否则无法保存磁盘映像文件，如果选择的分区可用空间不能存储映像文件时，则会提示没有足够的空间存储文件，此时重新选择另外的分区，以完成磁盘映像操作。

这里单击“High”按钮，提示是否执行操作，如图 6-49 所示。单击“Yes”按钮开始建立分区映像文件，如图 6-50 所示。

备份完成后，单击“Continue”按钮即可。至此，成功建立了磁盘分区映像文件，当已建立备份的分区数据受损时，用此映像文件还原即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

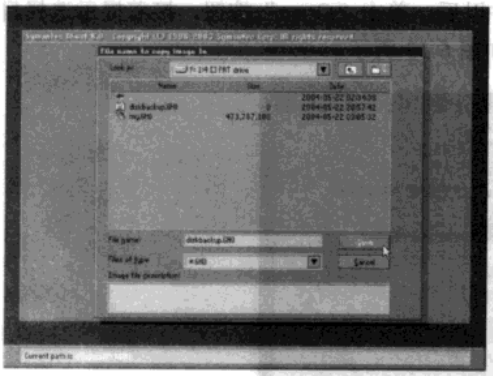


图 6-47

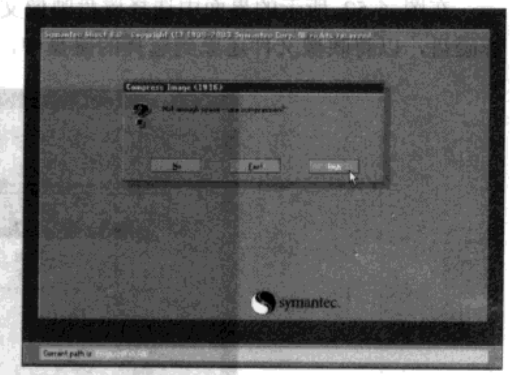


图 6-48

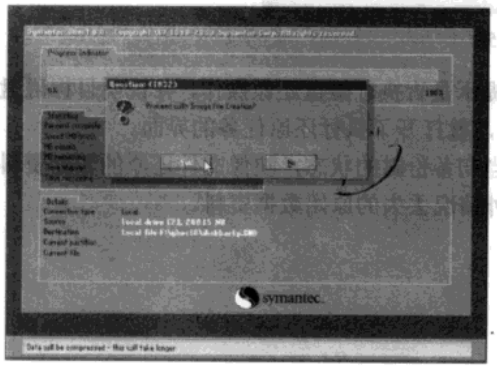


图 6-49

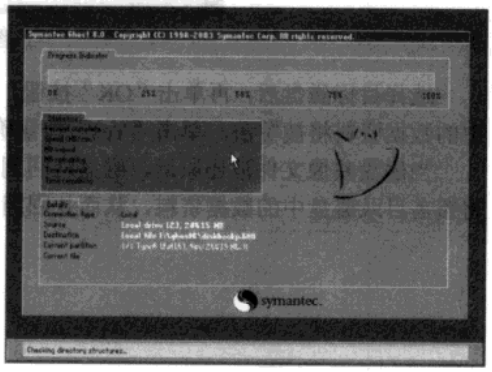


图 6-50

2．利用 Ghost 恢复磁盘映像

进入 Ghost 8.0 主界面，单击“Local”→“Disk”→“From Image”命令，如图 6-51 所示，Ghost 会提示选择磁盘映像文件，如图 6-52 所示。

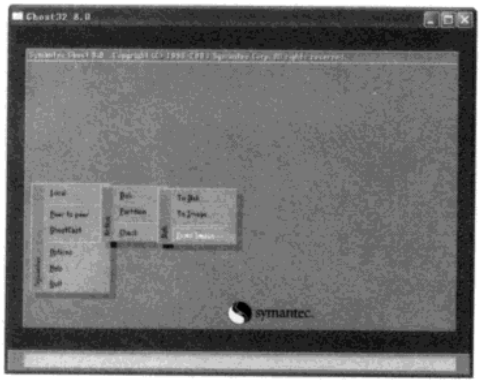


图 6-51

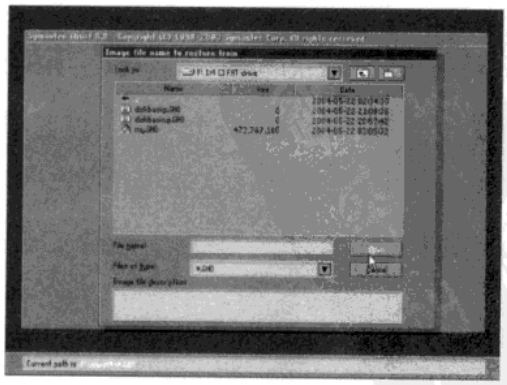


图 6-52

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在图 6-52 所示的界面中选择磁盘映像文件以后，单击“Open”按钮，接着提示选择目标磁盘，以将映像文件还原到选择的磁盘中，如图 6-53 所示。

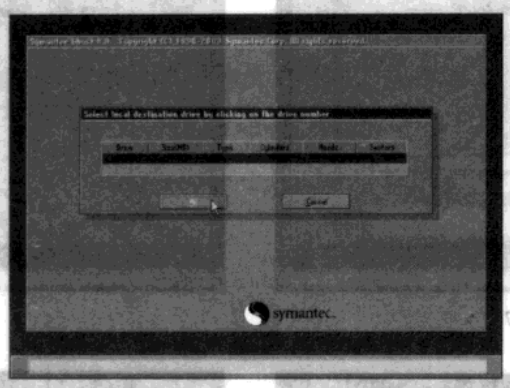


图 6-53

选择目标磁盘后，再单击“OK”按钮，将提示是否执行磁盘还原操作，并说明目标磁盘中的数据资料将被覆盖，单击“Yes”按钮确认，就打开了执行还原任务的界面。

当磁盘映像文件被还原后，磁盘就回到了当初备份时的状态，映像文件还原的数据资料将覆盖目录磁盘中的数据资料，从而找回因意外情况丢失的原始数据资料。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第7章 Windows 2000/XP/2003 故障恢复控制台经典救援经典案例

如果说 DOS 是 Windows 98 的“救命稻草”，那么也可以说故障恢复控制台是 Windows 2000/XP/2003 的“后悔药”。通过下面的案例，读者可学习通过系统恢复控制台来解决 Windows 2000/XP/2003 系统中所出现的故障，从而使系统更流畅地运行。

案例 52 用安装光盘引导进入恢复控制台

进入系统恢复控制台有两种方式：一种是通过安装光盘引导从安装模式选择系统恢复控制台方式（按 R 健），另一种是安装系统恢复控制台启动菜单。推荐使用前者，具体的操作步骤如下。

【第一步】开机时按 Del 键进入 BIOS，设置系统从 Windows 2000/XP 光盘启动。

【第二步】安装程序当进入到图 7-1 所示的安装界面，提示“要用‘恢复控制台’修复 Windows XP 安装，请按 R”，按“R”键进入系统恢复控制台。

【第三步】在图 7-2 所示的故障恢复控制台界面选择要登录的 Windows 安装，这里选择 2（这里因为安装了两个操作系统，所以有两个选项：“D:\WINNT”安装的是 Windows 2000，“E:\WINDOWS”安装的是 Windows XP）。

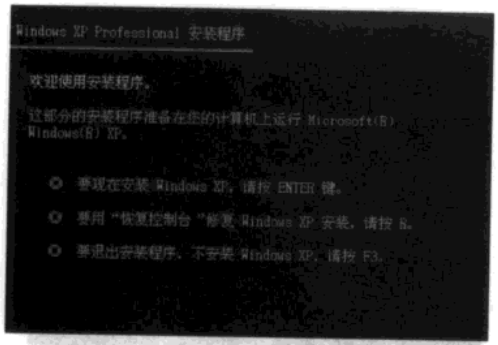


图 7-1

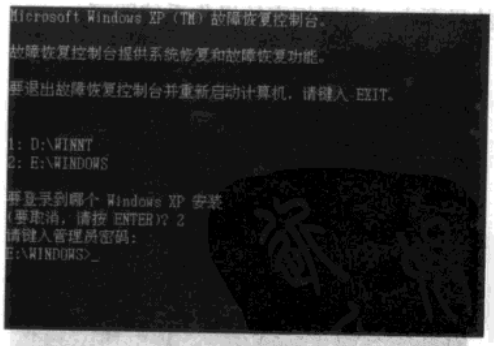


图 7-2

【第四步】键入正确的管理员（Administrator）密码；若管理员密码为空，直接按回车键即可进到 Windows 目录下。

【第五步】接下来就可以执行一些命令来恢复操作系统了。输入“help”按回车键可查看恢复控制台下可执行的命令。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

案例 53　安装恢复控制台为启动菜单项

若用户经常要使用恢复控制台，可以将恢复控制台安装到启动菜单项中。这样每次使用恢复控制台，只需要在计算机启动时，进入启动菜单中选择该选项即可。具体可以通过下面的操作步骤来完成。

【第一步】将 Windows 2000/XP 安装光盘插入光驱。若硬盘中有 Windows 2000/XP 安装文件，可以直接使用硬盘中的安装文件。

【第二步】在桌面左下角单击“开始”→“运行”命令。在“运行”对话框中单击“浏览”按钮，定位到光盘或硬盘安装目录下的\i386\winnt32.exe 处，并在后面加上“/cmdcons”参数，如图 7-3 所示。

【第三步】输入完成后单击“确定”按钮，这时程序询问用户是否安装恢复控制台。若安装，单击“是”按钮，如图 7-4 所示。安装程序开始复制一些文件到系统中，复制完毕后提示安装恢复控制台成功。

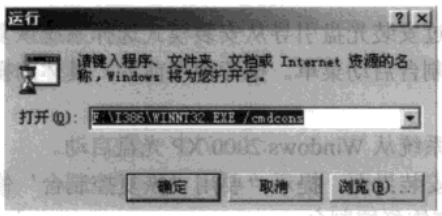


图 7-3

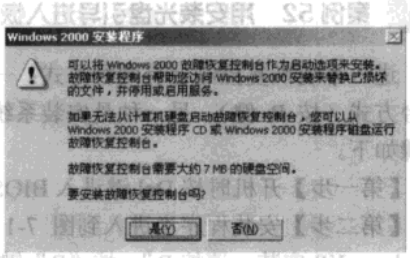


图 7-4

【第四步】重新启动计算机，在启动菜单里就可以看到“Microsoft Windows 2000 故障恢复控制台”选项，如图 7-5 所示。

【第五步】选择“Microsoft Windows 2000 故障恢复控制台”启动项后，进入图 7-6 所示的界面中，选择相应的操作系统即可。

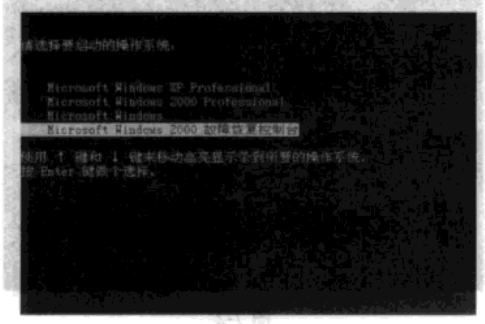


图 7-5

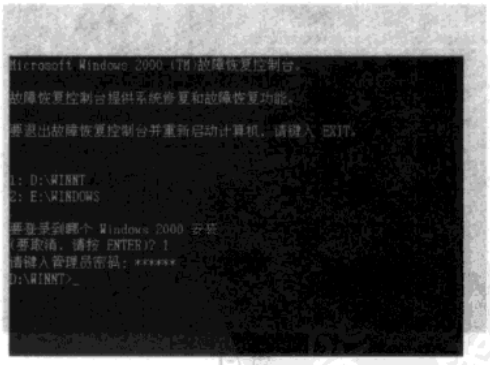


图 7-6

案例 54　系统启动时提示 ntfs.sys 文件丢失怎么办

在将分区从 FAT32 文件系统转换到 NTFS 文件系统之后，重新启动 Windows 2000/XP 时会出现“Missing or Corrupt ntfs.sys”（ntfs.sys 丢失或损坏）错误信息，导致系统无法正常启

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

动。此时不必紧张，也不必急着重新安装操作系统，可尝试通过 Windows 故障恢复控制台恢复该文件。

1. 在 Windows 2000 系统中

在故障恢复控制台下，使用 cd 命令进入“\winnt\system32\drivers”目录，在提示符后输入“ren ntfs.sys ntfs.old”，按回车键，将损坏的 ntfs.sys 文件重命名为 ntfs.old。

如果提示没有找到 ntfs.sys 文件，则说明该文件丢失了。此时把 Windows 2000 的安装光盘放进光驱，假设 Windows 2000 安装在 C 盘，先进入光盘的 i386 目录，如图 7-7 所示。

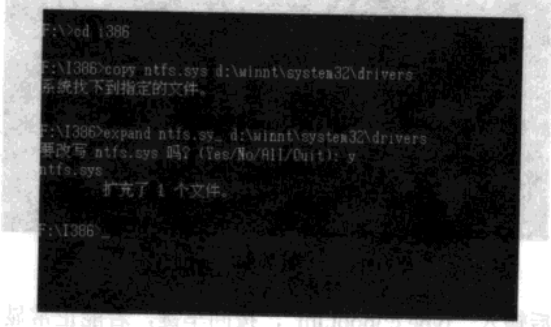


图 7-7

在提示符后输入“expand ntfs.sy_ d:\winnt\system32\drivers”，按回车键，把 ntfs.sy_文件拷贝到 d:\winnt\system32\drivers\下。

接着提示是否改写 ntfs.sys 文件。若改写，在提示后输入“y”，按回车键，开始复制文件。

文件复制完成后，退出故障恢复控制台，重新启动 Windows 2000 即可。

2. 在 Windows XP 系统中

在故障恢复控制台下使用 cd 命令进入\windows\system32\drivers 目录，接着运行指令“ren ntfs.sys ntfs.old”，将损坏的 ntfs.sys 文件重命名为 ntfs.old。如果提示没有找到 ntfs.sys 文件，则说明该文件丢失了。把 Windows XP 的安装光盘放进光驱，假设 Windows XP 安装在 C 盘，光驱的盘符为 H，键入“copy h:\i386\ntfs.sys c:\windows\system32\drivers”，按回车键，然后退出故障恢复控制台，重新启动 Windows XP 即可。

注意 在 Windows 2000 系统中，用户需要使用 expand 命令而不是 copy，因为要拷贝的文件还需要从压缩状态展开；而在 Windows XP 中则可以直接使用 copy，因为 ntfs.sys 直接存在。

案例 55 系统启动时提示 NTLDR 文件丢失怎么办

在 Windows 2000/XP 中都存在一个启动文件 NTLDR（这个文件无后缀名），该文件丢失会造成系统不能启动。如出现以下错误信息：NTLDR is missing, Press any key to restart。可以通过上面的办法从光盘或备份的安装文件中提取文件恢复(这里以 Windows 2000 系统为例)。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

进入故障恢复控制台，把 Windows 2000 的安装光盘放进光驱（设光驱盘符为 F:）。在提示符后输入“copy f:\i386\ntldr c:\”，按回车键，即从光驱复制 ntldr 文件至 C 盘根目录下。

接着，在提示符后输入“copy f:\i386\ntdetect.com c:\”，按回车键，即从光盘复制 ntdetect.com 文件到 C 盘根目录下。这时系统会提示是否覆盖文件，若覆盖，键入“y”，按回车键，如图 7-8 所示。

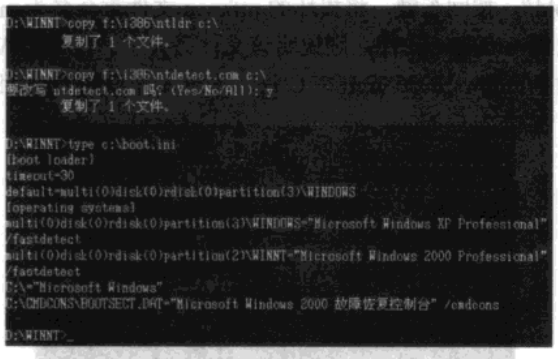


图 7-8

最后，在提示符后输入“type c:\boot.ini”，按回车键，若能正常显示 boot.ini 中的内容，则重启系统即可；若显示为“系统找不到指定的文件或目录”，那么意味着 boot.ini 文件损坏或丢失，可到其他安装 Windows 2000 的计算机中复制该文件，将它拷贝到 C 盘下，然后重启系统即可。

案例 56 误删了 SAM 文件怎么办

在 Windows XP 中如果不小心把 Windows\system32\config\下的 SAM 文件删除了，就会造成 Windows XP 账号丢失，不能进入 Windows XP 的登录界面。遇到这种情况，也可以通过控制台恢复文件，因为系统在最初安装 Windows XP 时备份过一个 SAM 文件在 C:\Windows\repair\sam 下，另外还有其他 4 个注册表文件，可以利用它们来恢复系统登录。具体操作步骤如下。

【第一步】删除损坏的包含密码信息的注册表文件。进入故障恢复控制台，进入 C:\Windows\system32\config 目录，在提示符后输入以下指令（假设系统安装在 C 盘）。

- delete c:\windows\system32\config\sam，如图 7-9 所示。



图 7-9

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- delete c:\windows\system32\config\system
- delete c:\windows\system32\config\software
- delete c:\windows\system32\config\security
- delete c:\windows\system32\config\default

【第二步】将 c:\Windows\repair\下的原始注册表文件拷贝到 c:\Windows\system32\config\位置，即依次执行以下指令。

- copy c:\windows\repair\system c:\windows\system32\config\system
- copy c:\windows\repair\software c:\windows\system32\config\software
- copy c:\windows\repair\sam c:\windows\system32\config\sam
- copy c:\windows\repair\security c:\windows\system32\config\security
- copy c:\windows\repair\default c:\windows\system32\config\default

【第三步】复制完成后，重新启动系统即可。

注意

由于 SAM 文件是当初安装 Windows XP 时产生的，而执行上面的操作则会丢失用户自己在系统中创建的用户和用户组(用户信息回到全新安装 Windows XP 时的状态)。但是，如果开了系统还原，可以先成功地登录 Windows XP，再还原到最新的还原点即可恢复全部用户设置。

另外，如果忘记了系统的登录密码，也可以利用此方案解决问题。

案例 57 多系统下 Windows XP 无法启动如何修复

为方便系统维护，很多用户安装了 Windows 98/2000/XP 多系统。正确的安装顺序是从低版本的 Windows 98 开始，然后依次安装 Windows2000、Windows XP。但是，如果先安装了 Windows 2000/XP，然后再安装 Windows 98，将导致 Windows 2000/XP 系统不能启动。

这种逆序安装会带来麻烦，但也不是不可修复。逆序安装后可按以下方法进行修复。

启动故障恢复控制台，在提示符后输入“bootcfg /add”，按回车键，将 Windows 安装添加到启动菜单列表中。

故障恢复控制台开始扫描 Windows 安装，扫描完成后，提示用户“选择要添加的安装”，如图 7-10 所示。

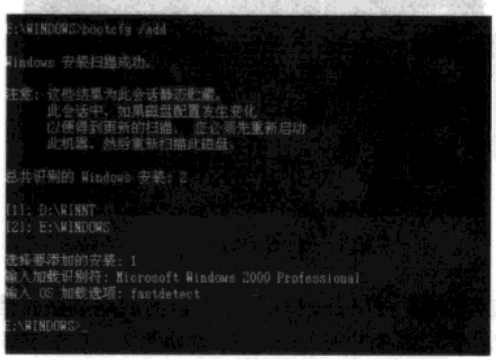


图 7-10

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如添加 Windows 2000 系统（在本例中装在 D:\WINNT 下），“输入 1”，按回车键。接着提示用户“输入加载识别符”，即启动菜单项名称，如上面恢复的是 Windows 2000 系统，可输入“Microsoft Windows 2000 Professional”，如图 7-10 所示。

接着按回车键，再次提示用户“输入 OS 加载选项”，直接输入“fastdetect”，按回车键。通过这样的操作，在启动菜单中就添加了 Windows 2000 系统的启动项。

如果还有 Windows XP、Windows 2003 系统，可以利用上面的方法继续在启动菜单中添加启动项，直至所有的系统都添加到多系统启动菜单为止。

最后，在提示符后输入“exit”，按回车键。重新启动计算机，就可以看到多系统启动菜单又回来了。以后就可以利用启动菜单项，方便地启动 Windows 2000、Windows XP 和 Windows 2003。

案例 58　误格式化 C 盘造成启动文件丢失怎么办

如果用户将系统安装到 C 盘之外的分区，很容易犯一个错误，即认为将系统安装到其他盘，C 盘的东西就都可以不要了。但事实并非如此，即使把操作系统安装到 C 盘之外的分区，系统所需要的一些引导文件仍然保留在 C 盘。如果此时将 C 盘格式化或将 C 盘上的文件全部删除，肯定会造成系统无法启动等严重问题。遇到这样的情况，可以通过恢复控制台来解决此类问题，具体的方法如下。

【第一步】进入恢复控制台后，在提示符后输入“bootcfg /add”，按回车键，重建 boot.ini 文件。

【第二步】在提示符后输入“copy f:\i386\ntdelect.com c:\”，按回车键，将 i386 目录下的 ntdetect.com 复制到 C 盘根目录下。

【第三步】在提示符后输入“copy f:\i386\ntldr c:\”，按回车键，将 i386 目录下的 ntldr 复制到 C 盘根目录下。

【第四步】在提示符后输入“fixboot c:，按回车键，向系统分区写入新的分区引导扇区。

【第五步】提示“确定要写入一个新的启动扇区到磁盘分区 C:吗？”，输入“y”，按回车键，提示“启动磁盘分区上的文件系统是 FAT32”，如图 7-11 所示。

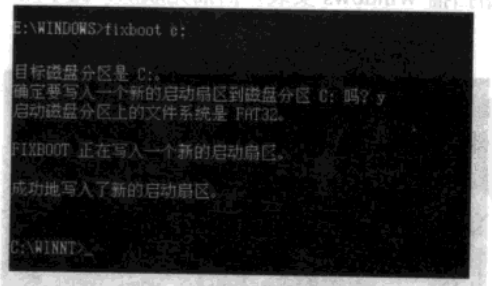


图 7-11

【第六步】接下来 FIXBOOT 程序开始写入一个新的启动扇区，当写入完成后，提示“成功地写入新的启动扇区”，表示新的启动扇区已经成功写入。

【第七步】退出恢复控制台，重新启动系统即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

案例 59 如何恢复损坏的 DLL 文件

Windows 2000/XP 不能启动、驱动程序文件损坏、重要系统文件丢失等情况都比较常见。要想知道具体丢失了哪些系统文件，读者可以在系统启动时按 F8 键进入高级选项菜单，选择“启用启动日志”选项，按回车键如图 7-12 所示。这样系统会自动在 C:\WINNT 目录下生成 ntbtlog.txt 文件，利用记事本可以打开 ntbtlog.txt 文件，看到如图 7-13 所示的信息。

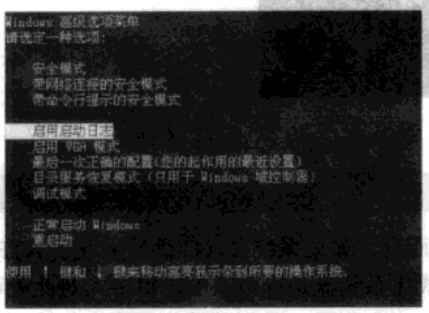


图 7-12



图 7-13

进入故障恢复控制台，输入“type ntbtlog.txt”，按回车键，这样就会显示该文件的内容。查看最后面的语句，如果语句中包含有“Fail”字符，那么将其后面的文件名记录下来，然后进行恢复。

例如系统提示 C:\WINNT\system32\下的 kbdal.dll 文件丢失，则在光盘中找到同名文件，然后在提示符后输入“copy f:\i386\kbdal.dll c:\WINNT\system32\”（F 为光驱盘符），按回车键，向 C:\WINNT\system32\复制 kbdal.dll 文件，这样就可以恢复丢失或损坏的 kbdal.dll 文件。

有些文件不能使用 copy 命令进行拷贝，或某一系列驱动程序丢失造成系统不能正常启动，这时可用 expand 命令来提取缺少的文件。

例如系统提示 C:\WINNT\system32\下 msr2c.dll 文件丢失，在安装光盘的 i386 目录中找到 msr2c 文件。然后，在提示符后输入“expand f:\i386\msr2c c:\WINNT\system32\msr2c.dll”，按回车键，即可恢复 msr2c.dll 文件。

案例 60 在恢复控制台下修复分区表

若当前用户只安装了 Windows XP 系统，且文件系统为 NTFS 格式，要在 DOS 下修复被损坏的分区表是比较麻烦的，这时可以使用 Windows XP 中的恢复控制台来进行修复。

进入故障恢复控制台后，在提示符后输入“fixmbr”，按回车键，接着出现一段警告信息，如图 7-14 所示。

然后提示“确实要写入一个新的主启动记录吗？”，输入“y”，按回车键，即可向主启动记录写入信息，如图 7-14 所示。

通过此操作可以恢复大多数分区表错误。使用 fixmbr 命令不仅可以修复 Windows XP 系统下的分区错误，对 Windows 98 系统，以及 Windows 98/XP 双系统也同样可以修复分区表。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

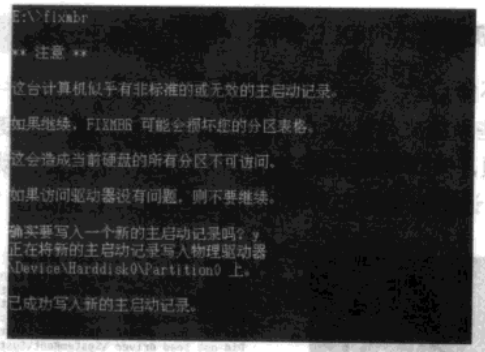


图 7-14

案例 61　如何格式化 NTFS 格式的系统盘

对于只安装了 Windows 2000 或 XP 系统的用户而言，如果系统盘（C 盘）采取了 NTFS 格式，想用 Windows 98 启动盘启动到 DOS 然后格式化系统盘是行不通的，很多人对此无可奈何。其实，除了使用 PM 等第三方工具来格式化 NTFS 分区，还可以进入故障恢复控制台中，利用 format 命令来对 NTFS 分区进行格式化。因为在故障恢复控制台下，可以识别 NTFS 分区。具体的操作如下。

进入故障恢复控制台，在提示符后输入“format c:”，按回车键，接着提示是否格式化 C 盘，如图 7-15 所示。

在“继续格式化吗（Y/N）？”后输入“y”，按回车键，即可开始进行格式，如图 7-15 所示。

格式化完成后，进入 C 盘下，会发现 C 盘中的数据已经不存在了，如图 7-16 所示。

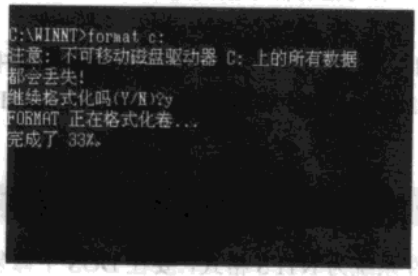


图 7-15

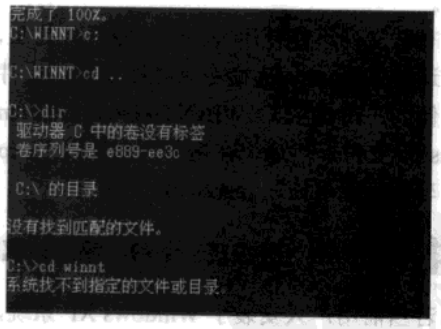


图 7-16

案例 62　如何从手动备份的注册表文件恢复注册表

在 Windows XP 中，注册表所对应的物理文件都保存在 Windows\system32\config 下（在 Windows 2000 中，此路径的 WINNT\system32\config），这里物理文件分别是 SYSTEM、SOFTWARE、SECURITY、SAM、DEFAULT 这 5 个文件，如图 7-17 所示。若注册表遭到破坏，可以在故障恢复控制台下将这些文件复制到原位置处，即可修复注册表。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

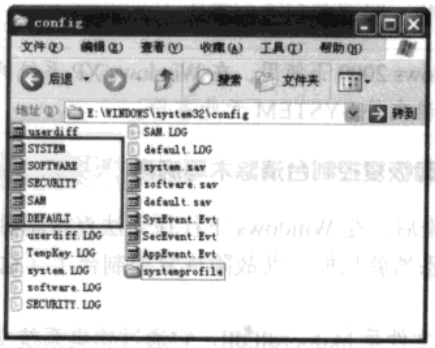


图 7-17

进入恢复控制台后，在提示符后输入以下指令（这里假设备份文件在 E\back\reg 下）。

- copy e:\back\reg \system c:\windows\system32\config\system
- copy e:\back\reg \ software c:\windows\system32\config\software
- copy e:\back\reg \ sam c:\windows\system32\config\sam
- copy e:\back\reg \ security c:\windows\system32\config\security
- copy e:\back\reg \ default c:\windows\system32\config\default

案例 63 如何从系统自动备份的注册表文件修复注册表

在 Windows 2000 C:\WINNT\system32\config 目录下的 5 个注册表文件中，SYSTEM 文件有一个备份叫 SYSTEM.ALT（如图 7-18 所示），它在系统启动时与 SYSTEM 同步生成，却不与 SYSTEM 同步改变。如果用户因改变了 SYSTEM 文件所对应的注册表编辑器 HKEY_LOCAL_MACHINE\SYSTEM 子键下的配置，导致系统无法启动，可启用此备份文件替换原文件修复系统。具体操作步骤如下。

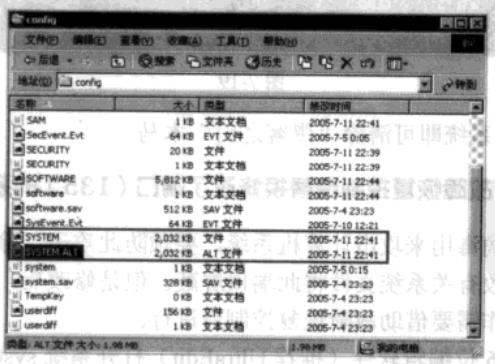


图 7-18

【第一步】进入故障恢复控制台，再进入 C:\WINNT\system32\config 文件夹下，在提示符后输入“rename SYSTEM SYSTEM.OLD”，按回车键，将 SYSTEM 文件改名为 SYSTEM.OLD。

【第二步】在提示符后输入“rename SYSTEM.ALT SYSTEM”，按回车键，将 SYSTEM.ALT 文件改名为 SYSTEM。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

【第三步】重新启动电脑，即可顺利进入系统。

注意 此法仅在 Windows 2000 下使用，在 Windows XP 系统的 Windows\system32\config 目录下的注册表文件 SYSTEM 无此备份。

案例 64 如何从故障恢复控制台清除木马病毒

系统被木马或病毒感染后，在 Windows 下往往无法直接删除病毒文件。如果在安全模式下也无法做到这一点，恐怕就只能借助故障恢复控制台了（这里以清除“黑客之门”木马为例）。

“黑客之门”的服务端文件是 hkdoordll.dll，它通过感染系统文件 services.exe 启动自身。用户只需删除此服务端，并使用正常的程序替换被感染的 services.exe 即可清除病毒。

【第一步】进入故障恢复控制台，如果用户使用的系统是 Windows XP 或 Windows 2003 Server 系统，在提示符后输入“copy f:\i386\services.ex_ C:\windows\services.exe”，按回车键，提取安装光盘中“健康”的 services.exe 文件来替换 C:\windows 下被感染的文件。

【第二步】如果用户使用是 Windows 2000 系统，在提示符后输入“copy services.ex_ e:\winnt\services.exe”，按回车键。系统提示“要改写 services.exe 吗？（Yes/No/All）”，在后面输入“y”，按回车键进行改写，如图 7-19 所示。

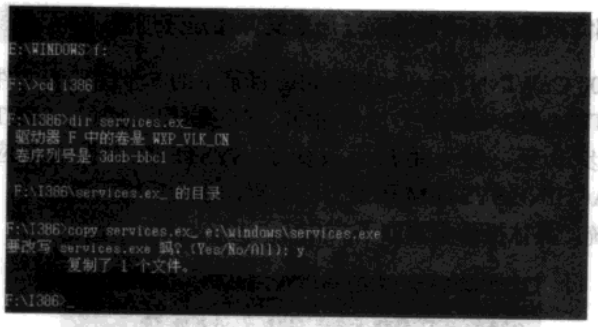


图 7-19

【第三步】重新启动系统即可清除“黑客之门”木马。

案例 65 如何从故障恢复控制台替换修改了端口（135）的系统文件

135 端口常被蠕虫病毒用来攻击计算机系统，要预防此攻击，除了需要下载微软的补丁程序外，还可以通过修改有关系统文件将此端口屏蔽。但是修改后，将无法直接在 Windows 下覆盖原文件，故此操作需要借助故障恢复控制台进行。

【第一步】用一款 16 位编辑软件（推荐 UltraEdit）打开系统 system32 目录下的 rpcss.dll 文件。

【第二步】查找 3100330035 所在位置，用 3000300030 来替换它。此替换的作用是将 135 端口改为 000。

【第三步】修改完成后进行保存。接着进入故障恢复控制台，用修改后的文件替换原系统文件，操作如图 7-20 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 7-20

【第四步】重新启动系统，使用 netstat -an 命令，可以看到 Windows 2000 下已经没有 135 端口了。在 Windows XP 系统下，虽然还有 TCP 的 135，但是 UDP 里面已经没有 135 端口了。

案例 66 如何解除故障恢复控制台操作限制

出于安全考虑，在故障恢复控制台环境下用户对硬盘的访问有诸多限制——只能访问根文件夹、Windows 系统文件夹、可移动存储介质，而且，只能把文件从可移动介质复制到硬盘，而不能把硬盘上的文件复制到可移动介质上。如果认为这些安全设置对自己作用不大，可解除这些限制，使系统恢复操作更加方便。

1. 设置安全策略

单击桌面上的“开始”→“运行”，输入“gpedit.msc”，打开组策略编辑器。依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”，在右侧窗口中找到“故障恢复控制台：允许对所有驱动器和文件夹进行软盘复制和访问”这个策略。

双击此策略，打开它的属性对话框，选择“已启用”选项。如果希望别人也可使用故障恢复控制台（不需要输入管理员密码），则须启用“故障恢复控制台：允许自动系统管理级登录”策略，如图 7-21 所示。

2. 修改环境变量

进入故障恢复控制台后，在提示符后输入“set”，按回车键，屏幕上将显示当前可用的环境变量，如图 7-22 所示。

接着，依次运行以下指令。

- set allowwildcards=TRUE，表示允许在某些命令中使用通配符。
- set allowallpaths=TRUE，表示允许更改目录来包括所有驱动器上的所有文件夹。
- set allowremovablemedia=TRUE，表示允许将硬盘上的文件复制到软盘或其他能识别的可移动载体上。
- set nocopyprompt=TRUE，表示在复制文件时，允许覆盖现有文件而不给出提示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 7-21

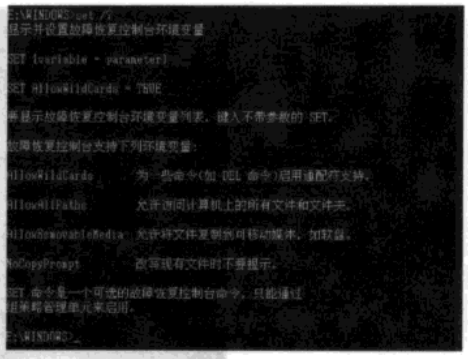


图 7-22

这样，故障恢复控制台的限制就被解除了。

案例 67　如何删除故障恢复控制台文件及启动菜单

虽然故障恢复控制台很好用，但如果用户不需要，可以手动将其删除。

【第一步】打开资源管理器，单击“工具”→“文件夹选项”→“查看”选项。在“高级设置”框下，选中“显示所有文件和文件夹”复选框和去除“隐藏受保护的操作系统文件”选项框，并单击“确定”按钮。

【第二步】进入 C 盘根目录，删除“\Cmdcons”文件夹、Cmldr 文件，如图 7-23 所示。

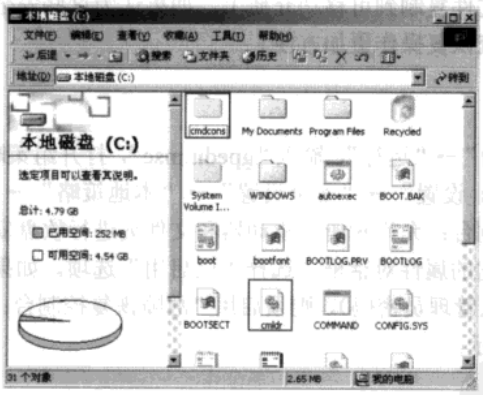


图 7-23

【第三步】选中 boot.ini 文件，单击右键，在弹出的下拉菜单中选中“属性”选项。在打开的“属性”对话框中清除“只读”复选框，单击“确定”按钮退出。

【第四步】利用“记事本”打开 boot.ini 文件，删除故障恢复控制台的条目（一般是“C:\cmdcons\bootsect.dat="Microsoft Windows Recovery Console"/cmdcons”），保存文件后关闭，最后再恢复 boot.ini 文件的只读属性即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第8章 Windows 窗口下的命令行

Windows 开始菜单中的“运行”命令是经常被用到的。从这里可以很方便地运行“开始→所有程序”菜单未列出的程序和命令，是程序菜单有益的补充。更出色的是，它允许在命令后面加上参数，如同在纯 DOS 中加参数运行命令一样。这意味着用户可以像在 DOS 下那样“精确”地运行 Windows 下的程序或命令。

“开始→运行”选项的应用实际是 DOS 思想的延伸。

与“开始→运行”选项具有相似功能的还有快捷方式，快捷方式指向的程序同样可以加入参数运行，巧妙运用能够起到一些意想不到的作用。

案例 68　如何快速启动系统自带的应用程序

在 Windows XP 下，用户一般要启动系统自带的某个应用程序（如“命令提示符”），都是通过单击“开始→所有程序→附件→“命令提示符”来启动。其实，可以从“开始→运行”窗口直接在“打开”框中输入“cmd”，如图 8-1 所示。单击“确定”按钮，即可弹出“命令提示符”窗口。

除了利用“运行”功能来快速启动系统自带的应用程序外，还可以利用它来启动用户自行安装的应用程序和要编辑的文档。通过单击“运行”窗口中的“浏览”按钮，可以指定要启动的应用程序和文档所在的路径，如图 8-2 所示，单击“确定”即可。

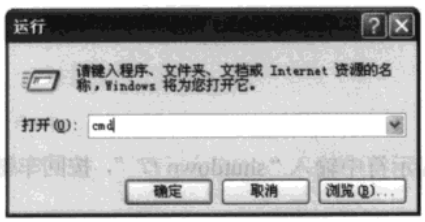


图 8-1



图 8-2

小知识

在 Windows XP 中，常用的可以通过“开始”→“运行”快速启动的系统应用程序如下。

devmgmt.msc ——打开设备管理器

dfrg.msc ——打开磁盘碎片整理程序

regedit.exe ——打开注册表编辑器

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

notepad	——打开记事本
calc	——打开计算器
gpedit.msc	——开组策略

案例 69　如何快速进入“准 DOS”窗口

“准 DOS”窗口与“命令提示符”有一定的相似，也有一定的区别。“准 DOS”窗口不支持长文件名和中文名，功能不如“命令提示符”强大；但是有一些命令只能在“准 DOS 窗口”才能运行，如 edit 命令，如图 8-3 所示。

那么如何才能快速地进入“准 DOS”窗口呢？很多读者都知道通过运行“cmd”命令可以弹出“命令提示符”窗口，如图 8-4 所示。而进入“准 DOS”窗口，则可以运行“command”命令，确定后即可弹出“准 DOS”窗口，如图 8-3 所示。

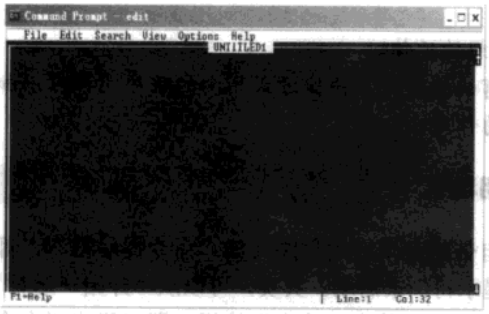


图 8-3

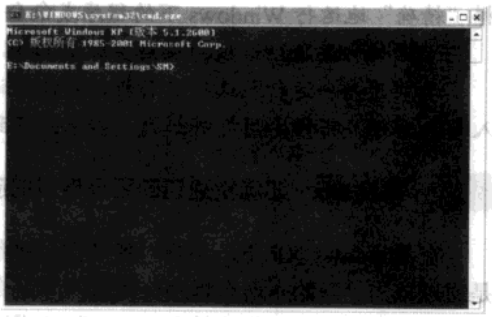


图 8-4

案例 70　如何手工定制“定时关机”指令

在 Windows 2000/XP 中，利用指令来关机需要调用 shutdown 命令，而该命令位于 \System32 文件夹下面。该命令的常用参数如下。

- -s：关闭计算机。
- -r：关闭并重启计算机。
- -a：放弃系统关机。
- -t：设置多长时间后关闭计算机。

若用户想了解此命令更多的使用参数，可以在提示符中输入“shutdown /? ”，按回车键，即可查看该命令详细的参数信息，如图 8-5 所示。

例如这里利用 shutdown 命令来设置计算机在 30 分钟后关闭，可以按如下方法来操作：在“运行”对话框的“打开”框中输入“shutdown –s –t 1800”（“1800”即 1800 秒），如图 8-6 所示。单击“确定”按钮后，弹出“系统关机”对话框，如图 8-7 所示。该对话框右上角的“关闭”按钮不可用，按 Alt＋F4 键也无效，进入任务管理器中也无法关闭此对话，因此颇有强制定时关机的意味。

如果需要取消关机命令，可以在“运行”对话框的“打开”框中输入“shutdown –a”，确定后可将此命令中止。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 8-5

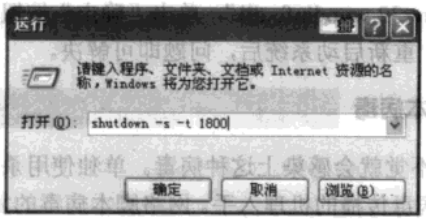


图 8-6

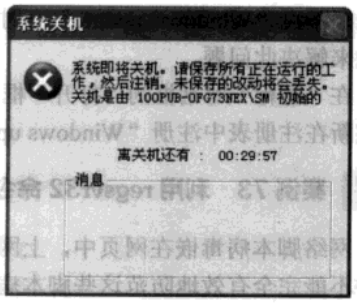


图 8-7

注意 -t 参数后的数字单位是秒，如果设置 30 分钟后关机，数字就应该是 30×60＝1800。

案例 71 利用 regsvr32 命令修复 IE 浏览器

一些系统文件丢失可能造成浏览器打不开新窗口，同时使用用鼠标右键中的“在新窗口打开”选也无效。要解决此问题，可以利用 regsvr32 命令来修复，具体操作如下。

【第一步】在“运行”对话框的“打开”框中输入“regsvr32 actxprxy.dll”。

【第二步】单击“确定”按钮，弹出一个对话框，提示“actxprxy.dll 中的 DllRegisterServer 成功”如图 8-8 所示。

【第三步】单击“确定”按钮，再次在“运行”对话框的“打开”中输入“regsvr32 shdocvw.dll”。单击“确定”按钮，弹出“shdocvw.dll 中的 DllRegisterServer 成功”提示信息，如图 8-9 所示。

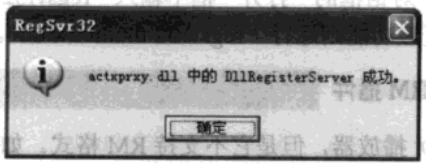


图 8-8



图 8-9

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

【第四步】单击“确定”按钮重新启动系统，即可修复 IE 浏览器。这时打开 IE 浏览器，在打开的网站中随意单击一个超链接，会发现 IE 可以在新窗口中显示超链接的页面内容了。

小提示

如果仍然不能解决问题，可以继续依次运行以下指令：

```
regsvr32 mshtml.dll
regsvr32 urlmon.dll
regsvr32 msjava.dll
regsvr32 browseui.dll
regsvr32 oleaut32.dll
regsvr32 shell32.dll
```

案例 72　利用 regsvr32 命令解决 Windows 无法在线升级的问题

Windows 的漏洞很多，每隔一段时间就需要使用“Windows update”升级程序进行在线升级。不过“Windows update”有时会出现无法使用的情况，这时，用户可以使用 regsvr32 命令来解决此问题。

在“运行”对话框的“打开”框中输入“regsvr32 wupdinfo.dll”，单击“确定”按钮，就会重新在注册表中注册“Windows update”组件。重新启动系统后，问题即可解决。

案例 73　利用 regsvr32 命令防范网络脚本病毒

网络脚本病毒嵌在网页中，上网时系统不知不觉就会感染上这种病毒。单独使用杀毒软件并不能完全有效地防范这些脚本病毒，必须从病毒传播的机理入手。网络脚本病毒的复制、传播都离不开 FSO（File System Object，文件系统对象），因此禁用 FSO 能有效地控制脚本病毒的传播。

在“运行”对话框的“打开”框中输入“regsvr32 /u scrrun.dll”，单击“确定”按钮即可禁用 FSO。如果要恢复 FSO，可以在“运行”对话框的“打开”框中输入“regsvr32 sorrun.dll”，单击“确定”按钮即可。

案例 74　利用 regsvr32 命令卸载 Windows XP 中不用的功能

Windows XP 系统功能强大，但也有些具体应用功能很简单，如 Windows XP 自带的 ZIP 功能远不如第三方软件强大，而且占用系统资源。为此，用户可以用 regsvr32 命令将这些不用的功能卸载掉。

在“运行”对话框的“打开”框中输入“regsvr32 /u zipfldr.dll”，单击“确定”按钮即可卸载 ZIP 功能。若要恢复 ZIP 功能，在“运行”对话框的“打开”框中输入“regsvr32 zipfldr.dll”，单击“确定”按钮即可。

同样用户要卸载图片预览功能，也可在“运行”对话框的“打开”框中输入“regsvr32 /u thumbvw.dll”，单击“确定”按钮即可。如果要恢复该功能则运行“regsvr32 thumbvw.dll”。

案例 75　利用 regsvr32 命令给 WMP 注册 RM 插件

很多朋友喜欢用 Windows Media Player（WMP）播放器，但是它不支持 RM 格式。如果用户想让 WMP 也能够播放 RM 格式的文件，用 regsvr32 命令注册一下 RM 插件即可（以

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



Windows XP 为例）。

【第一步】下载支持 RM 格式的插件——RealMediaSplitter.ax（下载地址：http://www.8boo.com/download/oldRealMediaSplitter.rar），解压缩后得到两个文件夹，分别是 Release（用于 Windows 98）和 Release Unicode（用于 Windows 2000/XP）。

【第二步】将 Release Unicode 文件夹下的 RealMediaSplitter.ax 文件拷贝到\Windows\System32 目录下。

【第三步】在“运行”对话框的“打开”中输入“regsvr32 RealMediaSplitter.ax”，单击“确定”按钮即可。

案例 76 利用 regsvr32 命令修复 Windows Media Player

Windows Media Player 播放器文件损坏，会出现“出现了内部应用程序错误”的提示，为了解决这个问题，用户可能会去重装系统。其实可以使用下面的方法来解决。

在“运行”对话框的“打开”框中输入“regsvr32 jscript.dll”，单击“确定”按钮将 javascript.dll 信息注册到注册表中。然后再次在“运行”对话框的“打开”框中输入“regsvr32 vbscript.dll”，单击“确定”按钮再将 vbscript.dll 信息注册到注册表中。重新打开 Windows Media Player 即可解决问题。

案例 77 利用 regsvr32 命令修复“添加/删除程序”无法启动的问题

在使用 Windows XP 系统时，用户可能会安装一些小程序，当不需要使用时就要将其删除，但是它们却没有卸载程序。这时就需要使用系统中的“添加/删除程序”来删除，但在双击“添加/删除程序”时又无法启动。遇到这样的情况，可以通过下面的方法来修复。

在“运行”对话框的“打开”框中输入“regsvr32 mshtml.dll”，单击“确定”按钮将 mshtml.dll 信息注册到注册表中。接着，再在“运行”对话框的“打开”框中输入“regsvr32 /i shdocvw.dll”，单击“确定”按钮将 shdocvw.dll 信息注册到注册表中。再次在“运行”对话框的“打开”框中输入“regsvr32 /i shell.dll”，单击“确定”按钮将 shell.dll 信息注册到注册表中。重新启动系统即可恢复。

案例 78 利用 certmgr 命令解决 EFS 加密文件夹无法打开问题

为了防止在重装系统后无法打开加密文件夹，用户可以通过下面的方法来备份和导入密钥，从而解决 EFS 加密文件夹无法打开的问题。

【第一步】在“运行”对话框的“打开”框中输入“certmgr.msc”，单击“确定”按钮打开“证书”管理器，如图 8-10 所示。

【第二步】展开“证书-当前用户”→“个人”→“证书”，这时在右侧的窗口中可看到本机所加密的文件夹。选中它并单击鼠标右键，在弹出的下拉菜单中单击“所有任务”→“导出”选项（如图 8-11 所示），进入“证书”导出向导，如图 8-12 所示。

【第三步】直接单击“下一步”按钮进入如图 8-13 所示的向导窗口，让读者选择“是，导出私钥”，还是“不，不要导出私钥”。

【第四步】选择“是，导出私钥”，单击“下一步”按钮进入如图 8-14 所示的向导窗口中，提示读者选择“导出文件格式”，这里用默认的导出文件格式。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 8-10

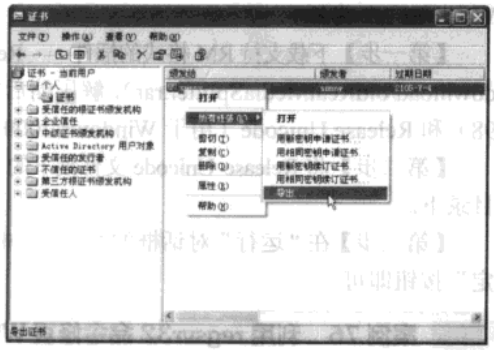


图 8-11

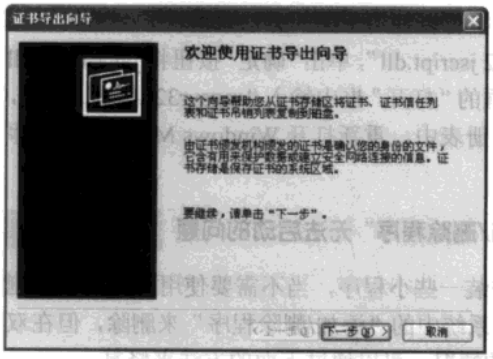


图 8-12

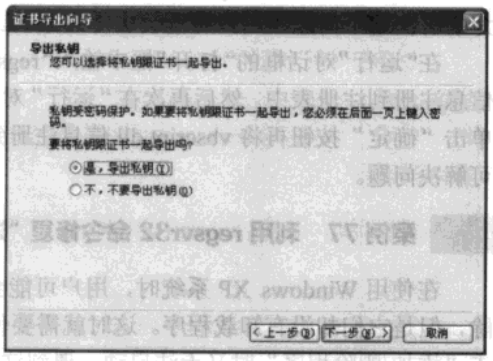


图 8-13

【第五步】单击“下一步”按钮进入如图 8-15 所示的向导窗口中，提示读者输入密码和确认密码。

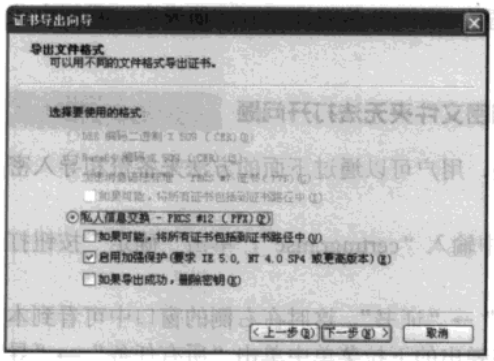


图 8-14

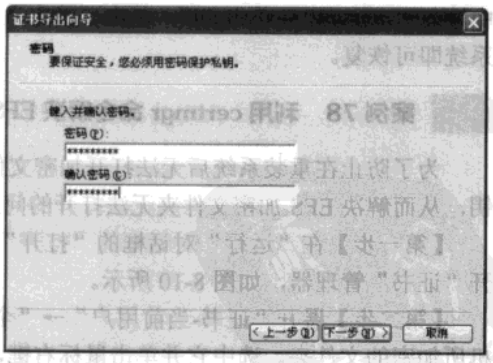


图 8-15

【第六步】输入完成后，单击“下一步”按钮进入如图 8-16 所示的向导窗口中，提示读者指定导出保存位置及文件名。

【第七步】为证书导出文件指定保存的位置和文件名后，单击“下一步”按钮进入如图 8-17 所示的向导窗口中，完成证书导出操作。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

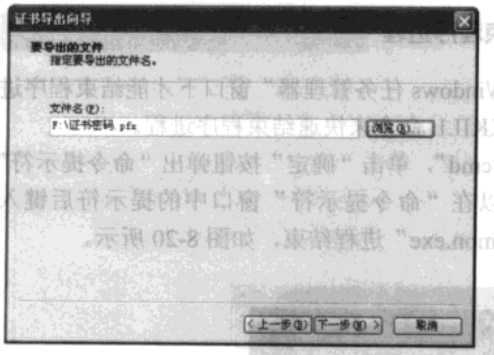


图 8-16

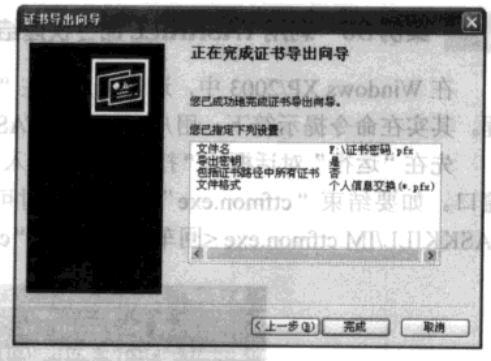


图 8-17

这样，在重装系统之后，找到导出私钥文件所保存的目录，右键单击导出的私钥文件，选择“安装 PFX”选项，如图 8-18 所示。系统会打开“导入私钥”向导（如图 8-19 所示），根据向导导入私钥。导入完成后，就可以顺利地打开 EFS 加密的文件夹。

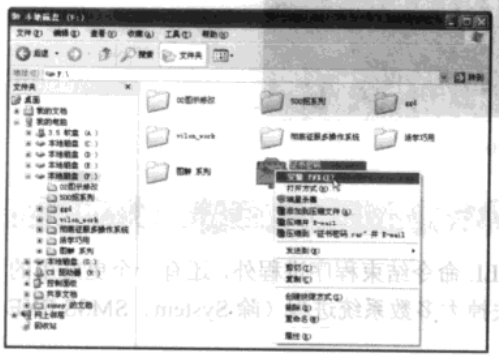


图 8-18

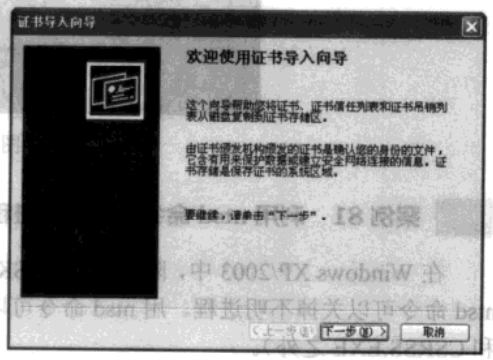


图 8-19

案例 79 利用 winword 命令快速恢复 Word 设置

经常使用 Word 的用户一般都会在工具栏中添加一些经常使用的功能，甚至将工具栏改变成符合自己习惯的样式。虽然这样的调整方便了自己的使用，但是对其他用户来说就有点不习惯了。要将工具栏恢复成原来的样子，可以通过下面的方法来实现。

在“运行”对话框的“打开”框中输入“winword /a”，单击“确定”按钮启动 Word，则所有界面都恢复到默认状态下。

小知识

这里向大家介绍 winword 命令最常用的参数以及参数的作用。

/t 模板名称：启动 Word，并打开基于非 Normal 模板的新文档，如/t Myfax.dot。

/a：启动 Word，并防止自动加载加载项和共用模板（包括 Normal 模板）。

/n：启动一个新的 Word 实例，并且不打开任何文档。

/w：启动一个含有空白文档的新的 Word 实例。

/m：启动 Word 时不运行任何 AutoExec 宏。

/m 宏名：启动 Word 时运行指定的宏。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

案例 80　利用 TASKKILL 命令快速结束程序进程

在 Windows XP/2003 中，通常用户要在“Windows 任务管理器”窗口下才能结束程序进程。其实在命令提示符下，用户可以利用 TASKKILL 命令来快速结束程序进程。

先在“运行”对话框的“打开”框中输入“cmd”，单击“确定”按钮弹出“命令提示符”窗口。如要结束“ctfmon.exe”进程，这时可以在“命令提示符”窗口中的提示符后键入 TASKKILL/IM ctfmon.exe <回车>，即可将“ctfmon.exe”进程结束，如图 8-20 所示。

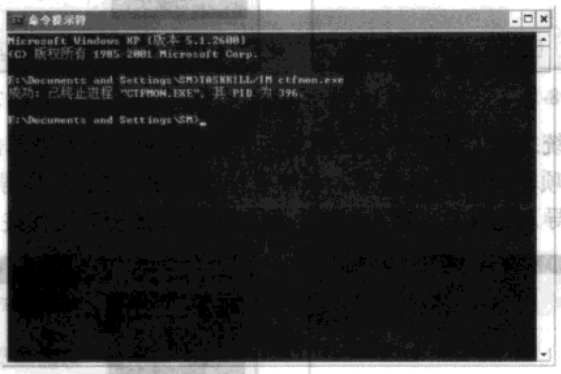


图 8-20

案例 81　利用 ntsd 命令关掉不明进程

在 Windows XP/2003 中，除了利用 TASKKILL 命令结束程序进程外，还有一个更好用的 ntsd 命令可以关掉不明进程。用 ntsd 命令可以关掉大多数系统进程（除 System、SMSS.EXE 和 CSRSS.EXE 之外）。

在关掉不明进程时，ntsd 会新开一个调试窗口，但一闪而过，用户几乎不能看清具体的过程。比如这里要关掉进程中的 CNNIC 中文网址更新程序（cdnup.exe），这时可以在提示符后输入“ntsd -c q -p 1268”（cdnup.exe 程序进程标示符），按回车键，即可将 CNNIC 中文网址更新程序（cdnup.exe）关掉，如图 8-21 所示。

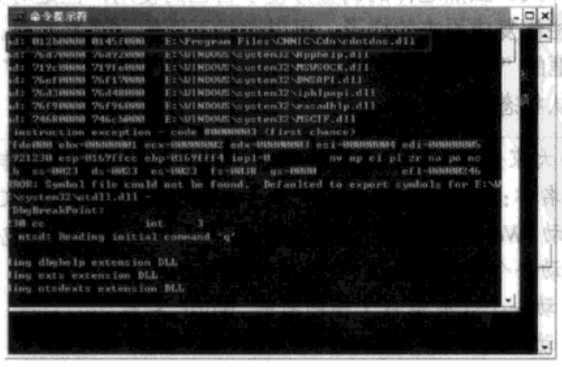


图 8-21

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

案例 82 解决组策略被禁用的问题

如果读者在组策略中设置了“只运行许可的 Windows 应用程序”（包括 gpedit.msc），却发现实际上组策略不能运行了。遇到此种情况，可以通过下面的方法来解决，让读者重返组策略。

【第一步】重新启动计算机时按下 F8 键，在 Windows 高级选项菜单里选择“带命令行提示的安全模式”进入。

【第二步】在提示符后输入“mmc”，按回车键，打开控制台窗口。

【第三步】单击“文件”→“添加/删除管理单元”，在“独立”选项卡中单击“添加”按钮，选择“组策略”管理单元，单击“添加”按钮；再依次单击“完成”→“关闭”→“确定”按钮，返回控制台；这样，添加的组策略管理单元将出现在控制台窗口中。

【第四步】找到被启用的设置，将其改回去（即设为“未配置”），如图 8-22 所示。



图 8-22

【第五步】按下“Ctrl＋Alt＋Del”组合键，选择关闭计算机，然后选择重新启动即可。

注意 在“带命令行提示的安全模式”中是看不到“开始”菜单和系统任务栏的。不过，用户可以键入“explorer”打开它们。

案例 83 彻底清除 3721 实名程序

读者有时想清除 3721 网络实名程序，但清除起来却很难。为此，读者可以尝试用如下方法彻底清除（这里以 Windows 2000 系统为例）。

【第一步】重新启动计算机时按下 F8 键，在 Windows 高级选项菜单里选择“带命令行提示的安全模式”进入。删除 C:\system32\drivers 目录下的 cnsminkp.dll 文件。

【第二步】同时按下“Ctrl+Alt+Del”组合键，调出“任务管理器”窗口。用“文件”下的新建任务命令，打开注册表编辑器。在注册表编辑器中，利用“查找”功能找到“CNSMIN.dll”所有项，并进行逐一删除。

【第三步】重新启动计算机，进入 Windows 系统。

【第四步】删除 C:\WINNT\dowloaded program files\下所有的文件和文件夹；删除 C:\Program

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Files\3721\下的所有文件和文件夹。

【第五步】用“Ctrl +Alt +Del”组合键调出任务管理器，建立新任务，运行注册表编辑器。删除键值含有“3721”的所有的项。

【第六步】按主机面板上的“Reset”按钮重启计算机。

案例 84　用 fc 命令破解 30 天共享软件使用限制

许多共享软件都有时间上的限制，到时间就不能再使用了。其中一些软件的共享限制是通过注册表完成的，程序每次启动之前，都会读取注册表进行比较，如果时间大于指定范围即过期了。那么如何才能从庞大的注册表中找到此子项呢？

第一次安装该软件时（30 天限制），可以打开注册表编辑器，选择“文件→导出注册表文件”选项，路径与文件名可自定义（如 c:\1.reg）。

之后，再将时间向前设置几天（如当天为 10 月 1 日，即改为 10 月 5 日）后，再运行一次此共享软件，其显示应为第五天，这时再次打开注册表编辑器并导出注册表文件（如 c:\2.reg）。

接下来在 Windows 的“命令提示符”下使用如下命令来比较这 2 个文件：fc c:\1.reg c:\2.reg>c:\ret.txt。

上述命令中的“>c:\ret.txt”为输出重定向，即让对比结果保存在文件中备用。比较过后，打开 C:\ret.txt，通过这个文件来找到共享软件暗藏在注册表中的共享限制的注册表子项。

案例 85　用 fc 命令辅助查杀 DLL 木马

在 Windows 2000/XP 系统中，system32 目录是木马隐身的常用地方，查找起来非常困难，DLL 木马尤其如此。针对这一点，用户可以在安装好系统和必要的应用程序后，对该目录下的 EXE 和 DLL 文件作一个记录。具体的方法如下。

打开“命令提示符”窗口，在命令提示符中进入 system32 目录下。接着在提示符后输入“dir *.exe>exeback.txt& dir *.dll>dllback.txt”，按回车键，这样所有的 EXE 和 DLL 文件的名称都分别被记录到 exeback.txt 和 dllback.txt 中，如图 8-23 所示。



图 8-23

日后如发现系统运行异常，使用杀毒软件又查不出问题时，就需要考虑一下系统中是否已经潜入 DLL 木马程序了。这时再次在提示符后输入“dir *.exe>exeback1.txt& dir *.dll>dllback1.txt”，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

按回车键，将当前 system32 目录下所有的 EXE 和 DLL 文件的名称都分别记录到 exeback1.txt 和 dllback1.txt 中。

然后在提示符后输入“fc exeback.txt exeback1.txt>diff.txt & fc dllback.txt dllback1.txt>diff.txt”，按回车键，利用 fc 命令比较前后两次所保存的文件，并将结果输入到 diff.txt 中。通过对这个文件进行查看，找到多出来的 DLL 和 EXE 文件，再通过查看创建时间、版本、是否经过压缩等，就能够比较容易地判断出是不是已经中了 DLL 木马了。接下来重新启动系统，进入安全模式下，逐一删除这些木马程序即可。

案例 86 利用 netstat 命令查看本机开放端口

netstat 是 Windows 自带的命令，可用于查看系统开放的端口，主要参数只有-a 和-n。前者表示显示所有连接和侦听端口，而后者表示以数字格式显示地址和端口号。

若用户想查看本机系统开放了哪些端口，可以在“命令提示符”窗口中输入“netstat –an”，按回车键，即可显示本机所有开放的端口，如图 8-24 所示。



图 8-24

Active Connections 是指当前本机活动连接；Proto 是指连接使用的协议名称；Local Address 是本地计算机的 IP 地址和连接正在使用的端口号；Foreign Address 是连接该端口的远程计算机的 IP 地址和端口号；State 则表示 TCP 连接的状态。

用户可以看到后面几行的监听端口是 UDP 协议的，所以没有显示状态。这里没有发现异常连接，表明系统是安全的。如果已知某木马使用的端口号，而此处发现该端口号是打开的并处于监听状态，那就可以判断系统中了哪种木马，如冰河木马的默认监听端口号为 7626。

案例 87 用 netstat 命令查找打开可疑端口的恶意程序

通过 netstat 程序可以查看系统开放的端口，但不能直接查看开放端口对应的程序。不过可以借助进程表示符 PID 和 tasklist 命令来查找可疑端口对应的恶意程序。

打开“命令提示符”窗口，在提示符后输入“netstat –ano”，按回车键，将显示当前活动端口及对应的进程标识（PID），如图 8-25 所示。

接着在提示符后输入“tasklist”，按回车键，将显示当前系统中正在运行的应用程序及其对应的进程标识。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

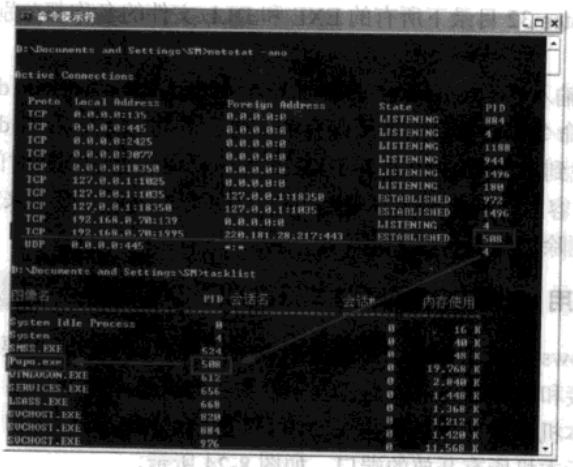


图 8-25

先从 netstat –ano 命令显示的结果找到可疑端口，然后根据其 PID 在 tasklist 命令中查找对应的程序，就能知道可疑端口对应的程序名了。从而判断可疑端口是否是恶意程序打开的（如图 8-25 所示），进而采取终止进程、删除恶意程序的安全措施。

案例 88　在 Windows XP 中用 netstat 命令直接查看端口与程序

在 Windows XP 中，netstat 还有一个增强的命令参数-b，利用它用户可以直接查看可疑端口和进程。

打开“命令提示符”窗口，在提示符后输入“netstat –anb”，按回车键，即可显示所有端口所对应的进程信息，如图 8-26 所示。

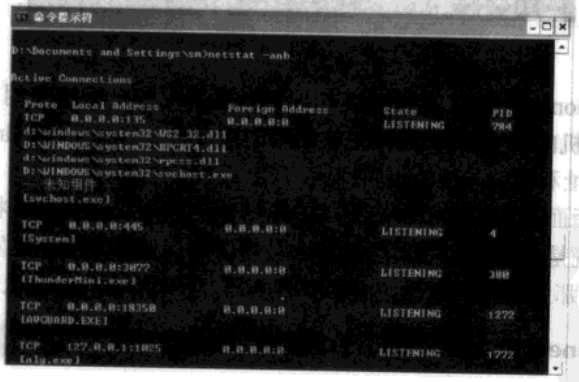


图 8-26

可以看出，每一个端口下面都列出了所对应的进程，查找木马程序非常方便。

案例 89　用 Fport 命令查看开放端口对应的程序

以上介绍了 Windows 自带的查看端口的命令行工具。常用的在命令行下运行的第三方端口查看工具还有 Fport（下载地址：http://www.foundstone.com/knowledge/zips/fport.zip）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Fport 是 FoundStone 出品的一个用来查看系统中所有打开的 TCP/IP 和 UDP 端口，以及它们对应程序的完整路径、PID 标识、进程名称等信息的小工具。下载并解压该工具，在命令行下进入其文件夹运行 Fport，如图 8-27 所示。

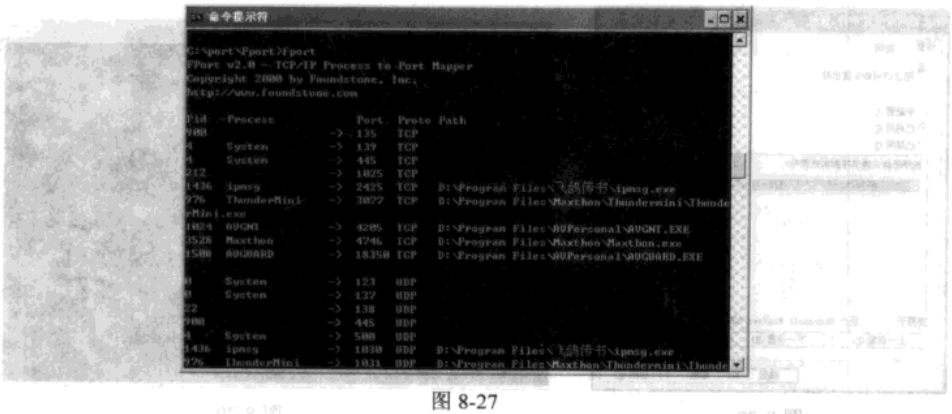


图 8-27

可以看到，系统开放的端口和对应的程序路径一目了然。这样，各个端口究竟是什么程序打开的，该程序的位置在哪里就清楚了。如果发现有某个可疑程序打开了某个可疑端口，一定要通过资料查证，确认不是恶意程序才能放过；否则将其删除。

案例 90 用 Subst 命令无软盘安装软件

在 Windows 9X/Me 系统中，Subst.exe 隐藏在\Windows\Command\下。如果是 Windows 2000/XP，则应该隐藏在\Windows\System32\下。

Subst.exe 的中文名称是“给目录赋驱动器符命令”，它的功能是以磁盘驱动器号代替路径名称，以使驱动器号与指定的子目录路径关联。其命令格式为：subst.exe [Driver1: [Driver2: Path]。其中的“Driver1”是指定指派路径的虚拟驱动器盘符，“Driver2 Path”则是指定物理驱动器和要指派给虚拟驱动器的路径。

在一些需要使用软盘的场合，用户可以先通过其他方式（例如 U 盘、局域网）将 A 盘的所有文件复制到本机的一个文件夹中，例如 D:\temp 下。接着在命令提示符窗口下键入命令“subst A: D:\temp”，然后用“dir A:”命令看看这里的文件列表是不是都在。按照这种方法将 D:\temp 文件夹虚拟成 A 盘，需要软盘的安装就可以顺利完成了。

注意 切记工作结束后一定要及时删除这个虚拟出来的 A 盘，否则无法正常使用原来的物理 A 盘。要删除这个虚拟出来的光驱时，只要执行“subst A: /D”命令就行了。

案例 91 停用“命令提示符”功能

有时为了安全起见，用户需要暂时停用“命令提示符”窗口的使用，此操作可以通过下面的步骤来实现。

在“运行”对话框的“打开”框中输入“gpedit.msc”，单击“确定”按钮打开“组策略编辑器”。接着，进入“用户配置”→“管理模板”→“系统”，在右侧找到名为“阻止访问

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

命令提示符”的策略。双击该策略，打开属性设置对话框，选择“已启用”复选框（如图 8-28 所示），这样就可以防止用户运行命令提示符。

以后用户进入“命令提示符”窗口后，会在“命令提示符”窗口中显示如图 8-29 所示信息。

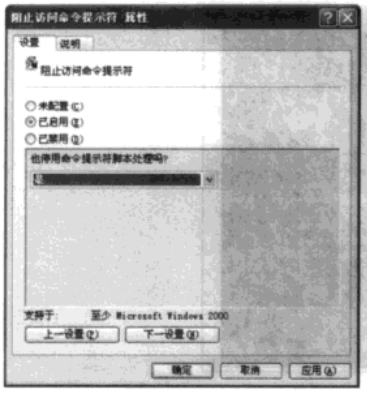


图 8-28

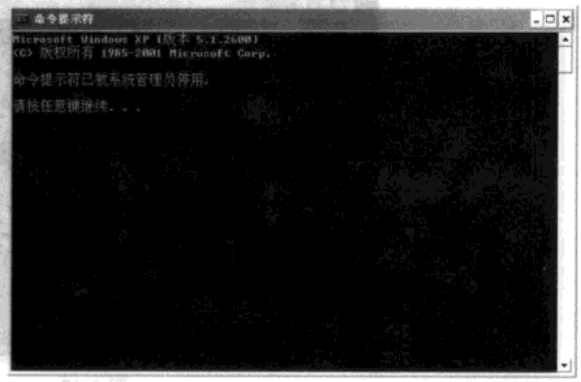


图 8-29

如果在图 8-28 中，将“也停用命令提示符脚本处理吗？”下选择“是”，还可以禁止批处理文件在系统上运行，这样就可以彻底禁止批处理文件对命令提示符的调用了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第9章 网络管理、维护经典案例

命令行在网络管理方面具有非常广泛和深入的应用，是网络管理员的好帮手；对于黑客而言，则是攻城掠地的利器。这些貌似平凡的命令行，在黑客手中似乎一下子拥有了神奇的能力，变得功能强大而又应用多彩了。

案例92 用ping命令诊断局域网故障

ping命令即ping.exe程序，是系统自带的用来进行网络连接测试的十分有用的工具，能准确快速地判断出网络故障。以某办公室的某台计算机为例：所用DNS服务器的IP地址为192.168.0.8，网关为192.168.0.8，本机IP为192.168.0.70，则通过如下测试可对网络状况做出判断。

1. 认识ping命令格式

```
命令格式：ping IP地址（或域名）-t -l -n
```

参数说明如下。

- -t：连续对IP地址执行ping命令，直到用“Ctrl+C”组合键中断。
- -l 3000：指定ping命令中的数据长度为3000字节，而不是缺省的32字节。
- -n：执行特定次数的ping命令。

2. 验证网卡工作正常与否

进入提示符窗口，在提示符后输入“ping 192.168.0.70”，按回车键，若出现如图9-1所示的信息，可以肯定当前网卡工作正常；若出现4行“Request timed out”提示，则说明网卡驱动程序或TCP/IP有问题，此时应该检查一下网卡驱动程序是否安装正确完好，TCP/IP协议是否正确安装。

3. 验证网络线路是否正常

在提示符后输入“ping 192.168.0.8”，按回车键，若出现如图9-2所提示信息，可以肯定网络线路畅通；若出现4行“Request timeout”提示，则说明网络线路有故障。

4. 验证DNS配置正确与否

在命令提示符窗口下ping一个著名的网站，比如新浪网www.sina.com.cn，如果正常的话，将会返回新浪网的IP地址，如图9-3所示。如果提示“Ping request could not find host www.sina.com.cn. Please check the name and try again”，则说明没有获得IP地址。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

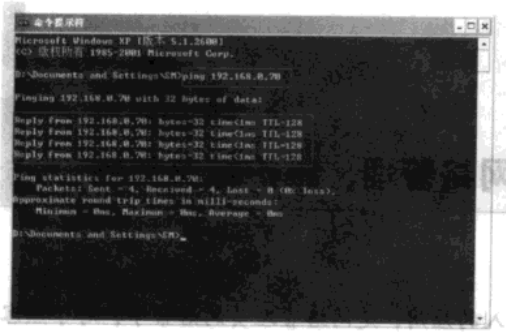


图 9-1

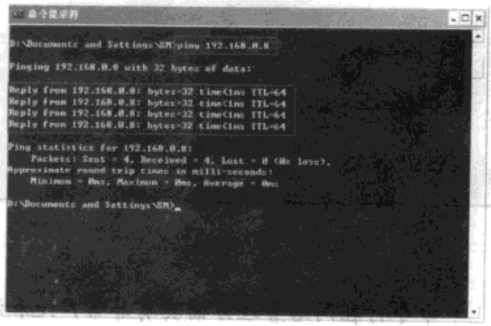


图 9-2

然后，再次在提示符后输入“ping 61.172.201.15”（ 新浪的一个 IP 地址），按回车键，看是否能够返回正确的结果。如果返回了正确的结果，则表明本机 DNS 服务器设置有问题。

案例 93 借用 ping 命令定时运行程序

ping 命令除了可以诊断局域网故障外，还可以利用 ping 的延迟参数让某个特定程序在特定的时间后运行。

在提示符后输入“ping 127.0.0.1 -n 10&net user netpatch2 /add”，按回车键，表示利用 ping 命令的-n 参数 ping 自己 10 下，ping 完后（20 分钟后）执行 net patch /add 命令，在本机系统添加 netpatch2 用户，如图 9-4 所示。

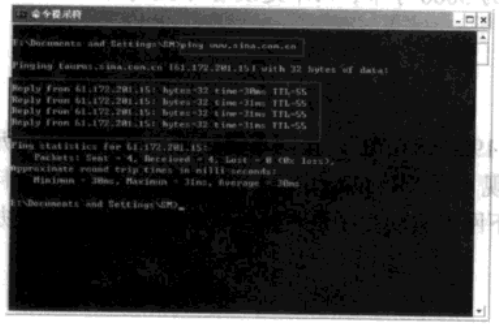


图 9-3



图 9-4

这样就达到了“定时”运行某程序（命令）的目的。

案例 94 用 tracert 命令了解本机与目标主机之间的数据传输路径

tracert 命令用来显示数据包到达目标主机所经过的路径，并显示到达每个节点的时间。命令功能同与 ping 类似，但它所获得的信息要比 ping 命令详细得多，它把数据包所经过的全部路径、节点的 IP 以及花费的时间都显示出来，该命令比较适用于大型网络。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1. 认识 tracert 命令格式

```
命令格式：tracert IP（主机名）[-d] [-h maximum_hops] [-j host-list] [-w timeout]
```

参数说明如下。

- -d：不解析目标主机的地址。
- -h maximum_hops：指定搜索到目标地址的最大跳跃数。
- -j host-list：按照主机列表中的地址释放源路由。
- -w timeout：指定超时时间间隔，程序默认的时间单位是毫秒。

2. 利用 tracert 命令了解本机与目标主机之间的数据传输路径

如用户想要了解自己的计算机与目标主机 www.sina.com.cn 之间详细的传输路径信息，可以在提示符后输入“tracert www.sina.com.cn”，按回车键，即可显示本机与 www.sina.com.cn 之间的数据传输路径信息，如图 9-5 所示。

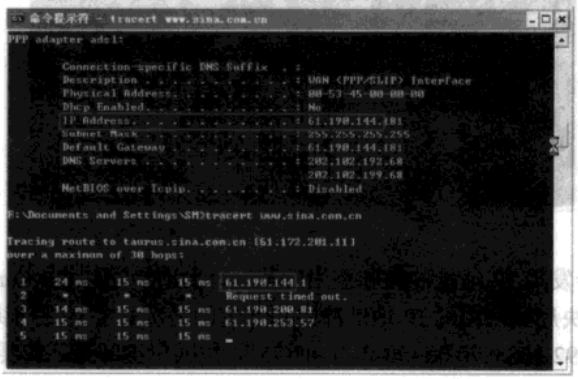


图 9-5

如果在 tracert 命令后面加上一些参数，还可以检测到更详细的信息。

案例 95 用 arp 命令查看哪些计算机连接了本机

在局域网中，用户可能很想知道哪些计算机与本机相连接。这里就需要在命令提示符状态下使用 arp 命令来实现。

1. 认识 arp 命令格式

```
命令格式 1：arp -a 或 arp  g
命令格式 2：arp -a IP
命令格式 3：arp -s IP 物理地址
命令格式 4：arp -d IP
```

功能说明如下。

- 命令格式 1：用于查看高速缓存中的所有项目。一般在 Windows 平台中使用 arp –a；而 arp –g 主要是在 UNIX 平台中。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 命令格式 2：此命令主要是针对于本机中有多块网卡时，使用该命令可以只显示与该接口相关的 ARP 缓存项目。
- 命令格式 3：向 ARP 高速缓存中人工输入一个静态项目。该项目在计算机引导过程中将保持有效状态，或者在出现错误时，人工配置的物理地址将自动更新该项目。
- 命令格式 4：使用本命令能够人工删除一个静态项目。

2. 利用 arp 命令查看哪些计算机连接了本机

在提示符后输入“arp –a”，按回车键，即可显示所有与本机相连接的计算机，并同时显示对方 IP 和 MAC 地址，如图 9-6 所示。

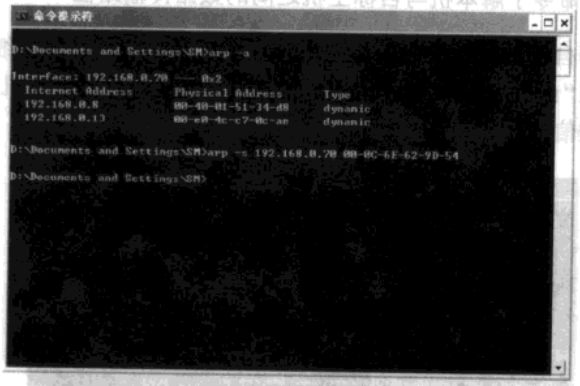


图 9-6

在局域网经常会发现 IP 地址冲突和盗用的情况，此时就可以利用 arp 命令来捆绑 IP 和 MAC 地址，从而解决局域网内的 IP 地址冲突和盗用的情况。要实现捆绑操作，只需要在提示符后输入“arp -s 192.168.0.70 00 -50-ff-6c-08-75”，按回车键即可。若要解除与网卡的 IP 与 MAC 地址的绑定，在提示符后输入“arp -d [网卡] 192.168.0.70”，按回车键即可。

案例 96 用 nbtstat 命令探测对方计算机名

当用户利用 arp 命令探测局域网内的一些与本机相连接的计算机后，却发现一些连接到本机的计算机不认识。那么要想知道这些不知名的计算机是何人在使用，可以在命令提示符状态下使用 nbtstat 命令来探测。

1. 认识 nbtstat 命令格式

```
命令格式：nbtstat -s -e -r -a -n
```

参数说明如下。

- -s：使用该参数从而按照各个协议分别显示其统计数据。如运行 Web 浏览器速度比较慢，或者不能显示 Web 页之类的数据，这时就可以用本选项来查看一下所显示的信息。通过查看找到出错的关键字，进而确定问题所在。
- -e：使用该参数主要用于显示关于以太网的统计数据。它会列出传送的数据包的总字节数、错误数、删除数、数据报的数量和广播的数量等信息。而且利用该选项可

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

以统计一些基本的网络流量。

- -r：使用该参数可以显示关于路由表的信息，类似于 route print 命令。除了显示有效路由外，还显示当前有效的连接。
- -a：使用该参数可以显示一个所有的有效连接信息列表，包括已建立的连接（Established），也包括监听连接请求（Listening）的那些连接。
- -n：使用该参数可以显示所有已建立的有效连接。

2．利用 nbtstat 命令探测对方计算机名

在提示符后输入“nbtstat -a 192.168.0.13”，按回车键，即可显示 IP 地址为 192.168.0.13 的计算机的信息，如计算机名称、在哪个工作组中，如图 9-7 所示。

案例 97 用 nslookup 命令解决上网故障

用户有时会遇到这样的问题，计算机能上 QQ，但利用浏览器浏览网页时却无法显示网页内容。这属于 DNS 服务器故障。用户可以在命令提示符状态下，尝试用 nslookup 命令解决问题。

1．认识 nslookup 命令格式

命令格式：nslookup 域名

功能说明：对指定的域名进行 DNS 测试，并反馈相关的信息，供用户查看找出问题所在。

2．查看 DNS 服务器工作是否正常

这里以新浪网（www.sina.com.cn）为例。在提示符后输入“nslookup www.sina.com.cn”，按回车键。如果 DNS 服务器工作正常，用户会看到如图 9-8 所显示的信息。

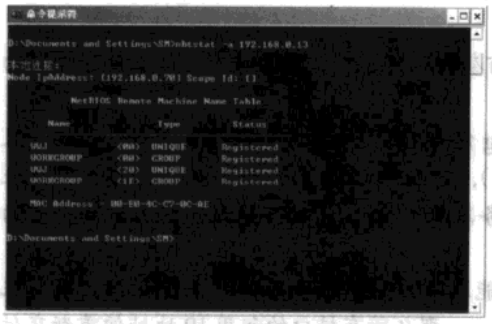


图 9-7



图 9-8

其中 Server 显示的是用户正在使用的 DNS 服务器域名；Address 表示 DNS 服务器 IP 地址；Name 表示查询域名的名称；Address 中出现了多个 IP 地址，证明该域名与多台服务器进行了绑定（一般大型站点才会如此）；Aliases 则是该域名的别名。

如果 DNS 服务器工作不正常，那么用户会收到“Can't find server name for domain. No response from server”提示信息，或者收到如下信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
-----------------------------------------------
***Defualt servers are no available
Server: Unknown
Address: 127.0.0.1
-----------------------------------------------
```

此时，应检查 DNS 配置是否正确。

3. DNS 服务器不能解析访问的域名

有时候可能会出现 DNS 服务器工作正常，却收到“Can't find www.xxx.com，No-existent domain”提示信息的情况。这表示该 DNS 服务器不能正常解析域名，访问被封掉的网站会出现这样的情况。

确定是 DNS 服务器故障引起的网页无法访问后，用户惟一能做的就是更换 DNS 服务器来解决。国内主要城市的 DNS 服务器列表可以到“http://www.router.net.cn/Article/Netadmin/nettech/200505/2375.html”中去查看。

案例 98 用 ipconfig 命令查看网络连接

ipconfig 是调试计算机网络的常用命令，通常用户使用它显示计算机中网络适配器的 IP 地址、子网掩码及默认网关。在 Windows 98 下面与此命令功能相同的程序是 winipcfg。

此命令的通常用法是加 all 参数，用以显示所有网络适配器（网卡、拨号连接等）完整的 TCP/IP 配置信息。

1. 认识 ipconfig 命令格式

```
命令格式 1：ipconfig
命令格式 2：ipconfig /all
命令格式 3：ipconfig /release 或 ipconfig /renew
```

功能说明如下。

- 命令格式 1：使用 ipconfig 时不带任何参数选项，它会显示每个已经配置了接口的 IP 地址、子网掩码和缺省网关值。
- 命令格式 2：使用此命令格式，ipconfig 能为 DNS 和 WINS 服务器显示它已配置且所要使用的附加信息（如 IP 地址等），并且显示内置于本地网卡中的物理地址（MAC）。如果 IP 地址是从 DHCP 服务器租用的，ipconfig 将显示 DHCP 服务器的 IP 地址和租用地址预计失效的日期。
- 命令格式 3：使用这 2 个命令格式，只能在向 DHCP 服务器租用其 IP 地址的计算机上起作用。如果用户输入 ipconfig /release，那么所有接口的租用 IP 地址便重新交付给 DHCP 服务器（归还 IP 地址）；如果用户输入 ipconfig /renew，那么本地计算机便设法与 DHCP 服务器取得联系，并租用一个 IP 地址。请注意，大多数情况下网卡将被重新赋予和以前所赋予的相同的 IP 地址。

2. 利用 ipconfig 命令查看网络连接状态

在提示符后直接输入“ipconfig /all”，按回车键，即可显示本机网卡的 IP 地址（192.168.0.1），

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

上网 IP 地址（61.190.144.94），如图 9-9 所示。

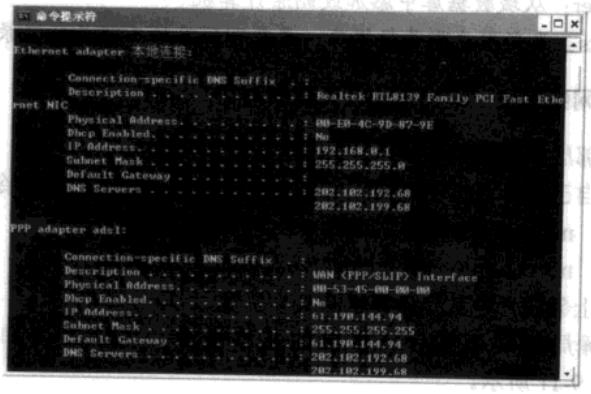


图 9-9

除此之外，还可以利用 ipconfig 来备份网络设置、为网卡分配新的动态地址等。

例如，在提示符后输入“ipconfig /batch bak-netcfg”，按回车键，即可将有关网络配置的信息备份到文件 bak-netcfg 中。

再如，在提示符后输入“ipconfig /renew 1”，按回车键，即可为网卡重新动态分配 IP 地址。

案例 99 善用强大的 net 命令

net 无论对于网络管理员还是黑客都是一个功能强大的命令。对于网管，应用得当可大大提高网络管理效率；对于黑客，Net 则成为攻城掠地的利器。

1. 认识 net 命令的格式

命令格式：net [accounts | computer | config | continue | file | group | help | helpmsg | localgroup | name | pause | print | send | session |share | start | statistics | stop | time | use | user | view]

- net view：显示域列表、计算机列表或指定计算机的共享资源列表。
- net user：添加或更改用户账号或显示用户账号信息。
- net use：连接计算机或断开计算机与共享资源的连接，或显示计算机的连接信息。
- net time：使计算机的时钟与另一台计算机或域的时间同步。
- net start：启动服务，或显示已启动服务的列表。
- net pause：暂停正在运行的服务。
- net continue：重新激活挂起的服务。
- net stop：停止 Windows NT/2000/2003 网络服务。
- net share：创建、删除或显示共享资源。
- net send：向网络的其他用户、计算机或通信名发送消息。
- net localgroup：添加、显示或更改本地组。
- net group：在 Windows NT/2000/2003 Server 域中添加、显示或更改全局组。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- net config：显示当前运行的可配置服务，或显示并更改某项服务的设置。
- net computer：从域数据库中添加或删除计算机。
- net accounts：更新用户账号数据库、更改密码及所有账号的登录要求。

2．net命令在网络管理、维护中的经典应用

（1）在“网上邻居”中隐藏本机

若用户不希望自己的计算机在“网上邻居”出现，可以使用如下命令。

- 隐藏命令：net config server /hidden:yes。如图9-10所示。
- 开启命令：net config server /hidden:no。如图9-10所示。

（2）查看“网上邻居”中某台计算机的共享资源

若用户想了解局域网上某台计算机的共享资源，可以使用如下命令：net view 192.168.0.16。如图9-11所示。

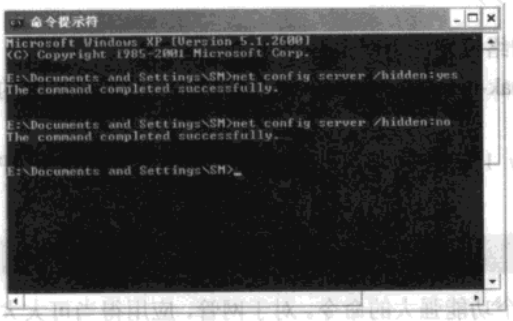


图9-10

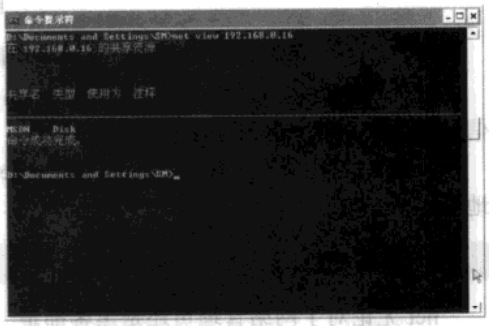


图9-11

（3）查看本机上的共享资源

若用户想了解本机到底共享了那些资源供局域网用户访问，可以使用如下命令：net share。如图9-12所示。

（4）手工删除本机共享

当了解了本机共享资源后，希望将一些共享资源不再共享，可以使用如下命令：

- 删除c$共享资源命令：net share c$ /d。如图9-13所示。
- 删除d$共享资源命令：net share d$ /d。如图9-13所示。

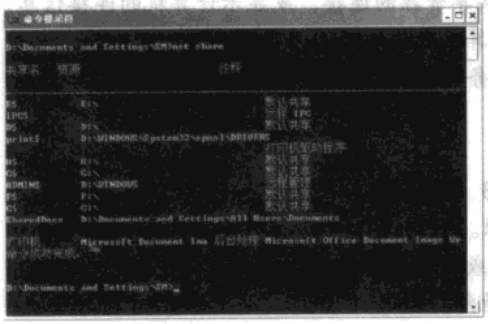


图9-12

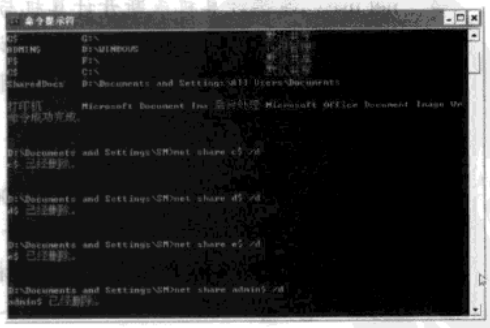


图9-13

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 删除 ipc$共享资源命令：net share ipc$ /d。如图 9-13 所示。
- 删除 admin $共享资源命令：net share admin$ /d。如图 9-13 所示。

注意 “$”符号后必须有空格符，再输入“/d”参数。

（5）建立远程 IPC$连接

与远程主机建立 IPC$连接为黑客常用的攻击手法。当拥有了远程计算机的用户名（例如 administrator）和密码时，就可以成功建立远程连接，进而映射磁盘，上传木马。

不过要建立远程 IPC$连接，必须知道对方计算机的 IP 地址。然后在提示符后输入“net use \\192.168.0.70\IPC$ "******" /user:administrator”，按回车键，如图 9-14 所示。

（6）映射远程机器的共享资源

如用户想映射远程主机 192.168.0.70 上的共享资源 C$为本地的 Z 盘，可以使用如下命令：net use z: \\192.168.0.70\C$。

注意 必须先建立 IPC$连接，这个命令才能成功使用。

（7）增加一个共享

用户可以在局域网中增加一个共享文件夹，以便于“网上邻居”中的用户访问。这里假设共享文件夹为 e:\download\movie，共享名为 mymovie，限制连接用户数为 1。这时可以使用如下命令：net share mymovie=e:\download\movie /users:1。如图 9-15 所示。



图 9-14



图 9-15

（8）查看本机中的用户账户列表

若用户想查看自己使用的计算机到底创建了多少个用户账户，可以使用如下的命令：net user。即可在列表中显示本机中所有的用户账户，如图 9-16 所示。

（9）添加新账户

若想添加一个新的用户账户，假设用户账户为 hacker，账户密码为 123456。可以使用如下命令：net user hacker 123456 /add。如图 9-17 所示。

（10）把账户添加进系统管理员组

默认情况下添加的用户账户是“受限”权限用户，而要把上面添加的“hacker”账户加入系统管理员组（即提升 hacker 的权限为管理员），可以使用如下命令：net localgroup administrators hacker /add。如图 9-17 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 9-16



图 9-17

（11）禁用系统的账户

若禁用 hacker 这个账户，使这个用户不能再登陆此计算机，可以使用如下命令：net user hacker /active:no。如图 9-17 所示。

（12）激活已禁用账户

若将禁用的账户激活，如上面的 hacker 账户，可以使用如下命令：net user hacker /active:yes。如图 9-17 所示。

（13）删除一个账户

若计算机中的有些账户已经没有用，这时可以将其删除掉，如删除 hacker 账户，可以使用如下命令：net user hacker /del。

（14）开启和关闭系统服务

Windows 系统中有很多有用或者无用的系统服务，有用的系统服务如果没有开启，将不能执行与服务相关的功能；而无用的系统服务如果不关闭，将占用系统资源。所以根据情况适当的开启或关闭系统服务是十分有必要的。

下面以 telnet 服务为例，介绍该系统服务的开启和关闭命令。开启 telnet 服务命令：net start telnet。如图 9-18 所示。关闭 telnet 服务命令：net stop telnet。如图 9-18 所示。



图 9-18

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
net start                                  //可开启的服务
net start alerter                          //启动报警服务
net start "compute browser"                //启动计算机浏览器服务
net start "dhcp client"                    //启动 DHCP 客户服务
net start event log                        //启动事件日志服务，用于记录本地计算机
                                             上的事件
net start messenger                        //启动信使服务，向计算机发送消息
net start ole                              //启动对象连接嵌入服务
net start "remote access connection manager" //启动远程访问连接管理服务
net start "remote procedure call(rpc) service" //启动远程过程调用（RPC）服务
net start schedule                         //启动计划任务服务
net start server                           //启动服务器服务，可以使用硬盘资源共享
net start snmp                             //启动 SNMP 服务，向 SNMP 管理系统报告
                                             当前状态
net start "remote registry"                //启动远程注册表服务
net start spooler                          //启动后台打印机程序
net start "tcp/ip netbios helper"          //在 TCP 服务上启用 NetBIOS 支持
net start ups                              //启动不间断电源 ups 服务
net start workstation                      //启动工作站服务，工作站服务是用计算机
                                             可以直接使用网络资源
net start telnet                           //启动 telnet 服务，打开 23 端口
net start lanmanserver                     //打开 IPC 服务
net start msftpsvc                         //打开 FTP 命令
net start termservice                      //启动 Windows 2000 的终端控制
net start smtpsvc                          //启动 SMTP 日志记录
```

小知识

注意 如果服务名称中带有空格，即由 2 个以上的词组合在一起，如“remote registry”，必须使用引号。

案例 100 了解 at 命令是如何启动木马程序的

黑客入侵后都会留下后门，也就是向入侵的计算机种入木马程序。那么在命令提示符中，是如何把木马传上去又如何启动的呢？实现木马上传、启动就需要利用 at 命令（假设这里已经登录了对方服务器）。

1. 认识 at 的命令格式

```
命令格式 1: at [\\computername] [ [id] [/delete] ]
命令格式 2: at [\\computername] time "command"
```

- \\computername：要设置任务的计算机名或 IP 地址。
- id：任务号。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- /delete：删除任务。
- time：设置任务运行时间。
- command：设置运行的程序（命令）。

2. 用 at 命令启动木马程序

用 at 命令启动木马程序首先要得到对方计算机的时间。在提示符后输入“net time \\61.190.144.86”，按回车键，此命令将会返回对方计算机的时间，这里假设时间为“12:11”。现在就新建一个启动远程计算机程序的任务，假设 IP 地址为 61.190.144.86，运行程序为 admin.exe。这时就可以使用如下命令：at \\61.190.144.86 12:13 admin.exe。这里假设了一个服务端木马，即 admin.exe，这个木马要事先放在对方计算机的系统目录下面；“12:13”为设置木马运行的时间。

这样，等到了 12:13 就可以从客户端向服务端发出连接请求，连接上之后就可以实施远程控制了。

案例 101 用 at 命令设置计划任务

at 命令除了被黑客作为不法的操作外，还可以利用它对计算机进行管理操作，如定时关机、定时提醒、自动运行批处理文件、取消已经安排的计划等操作。

1. 定时关机

要实现定时关机操作，只需要在提示符后输入“at 21:00 shutdown -s –t 30”，按回车键，表示到了 21:00 点钟，电脑会自动弹出“系统关机”对话框，并默认 30 秒延时自动关机。

2. 定时提醒

要实现定时提醒，只需要在提示符后输入“at 12:00 net send 10.10.36.122 下班时间到，不要忘记签退!!”，按回车键，表示到了 12:00 点钟，电脑会自动向 IP 地址为“10.10.36.122”的计算机发送“下班时间到，不要忘记签退!!”的信息，如图 9-19 所示。



图 9-19

小知识 这里的 net send 是 Windows 内部程序，可以向局域网内的任意计算机发送消息，该功能在 Windows 中也称作“信使服务”。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3. 自动运行批处理文件

要在特定的时间运行某个特定的批处理文件，可以在提示符后输入“at 1:00AM /Every:Saturday backup.bat”，按回车键。表示在每个 Saturday（周六）的早上 1:00 点，电脑定时启动 backup.bat 批处理文件。

backup.bat 可以是用户自行编制的批处理文件，也可以是用户在批处理文件中添加有用的指令，如自动对数据进行备份等指令。也可以自选编制一个开机批处理文件。

4. 取消已经安排的计划

有时候用户已经安排好的计划，可能因其他事情而临时变动，此刻就需要提前改变计划或取消计划。这时在提示符后输入“at 5 /delete”，按回车键即可，而这里的“5”是安排计划时所指派给已计划命令的标识编号，如图 9-19 所示。

案例 102 用 telnet 命令远程连接计算机

此命令对黑客非常实用，用此命令可以与远程计算机连接，正常情况下需要用户名、密码。

1. 认识 telnet 命令格式

命令格式：telnet [host [port]]

功能说明如下。

- hst：指定要连接到的 IP 地址。
- prt：要连接到的端口号。

2. 连接木马开放端口

如果黑客已经通过某种途径使对方运行了自己的木马（比如通过 QQ 发送具有欺骗性的木马程序），就可以直接连到这个木马打开的端口。假设木马的服务端口是 99，可以使用如下命令：telnet 127.0.0.1 99。这样就连到了方的 99 号端口，可以在对方计算机运行命令，如图 9-20 所示。

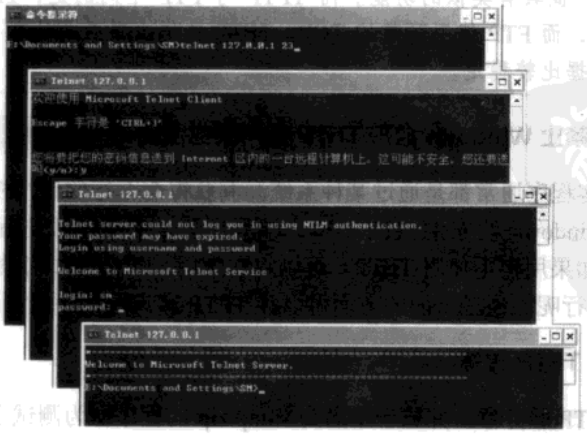


图 9-20

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

案例 103　用 FTP 命令传输文件

FTP 命令可以将用户的东西传到对方计算机上去。如果用户已经申请了支持 FTP 上传的空间，那么会得到该空间的用户名、密码以及 FTP 服务器地址。接下来就可以利用 FTP 命令来上传文件到该空间。

1. 认识 FTP 命令格式

```
命令格式：FTP -v -d -i -n -g [主机名]
```

参数说明如下

- -v：显示远程服务器的所有响应信息。
- -n：限制 FTP 的自动登录。
- -d：使用调试方式。
- -g：取消全局文件名。

2. 利用 FTP 命令上传文件

在上传之前，用户需要知道上传的 FTP 服务器地址、用户名和密码。这里假设 FTP 服务器为 www.ftp.net、用户名为 hack、密码为 654321。下面来看看具体的上传文件操作：

首先，在提示符后输入“FTP www.ftp.net”，按回车键，提示用户输入用户名和密码。

接着，根据提示信息输入用户名（hack）和密码（654321），并按回车键。

接下来就是上传文件，假设用户需上传的文件是 index.htm，它位于 C:\下，传到服务器计算机的 D:\下，这时在提示符后输入“get c:\index.htm d:\”，按回车键，即可开始上传文件。

若用户想将空间中的文件下载到本地计算机上，假如把 FTP 空间中的 C 盘下的 index.htm 下载到用户计算机的 D 盘下，这时在提示符后输入“put c:\index.htm d:\ ”，按回车键，即可开始下载文件。

小知识　除了可以使用 FTP 命令从空间上上传和下载文件外，另一个文件传输工具 TFTP 也具有类似的功能。而 TFTP 与 FTP 不同的是，TFTP 使用不可靠的 UDP，而 FTP 使用可靠的 TCP。TFTP 传送少量数据比较方便，FTP 传送大量数据比较稳定。

案例 104　禁止 Windows 自带 TFTP 客户端的使用

网络蠕虫或黑客程序通常都是通过某种系统漏洞获得命令行的运行权限，在此过程中，蠕虫往往是借助 Windows 自带的 TFTP 客户端程序获取必要的攻击程序或后门程序，如 iishack、nc 之类。如果用户不使用 TFTP，可以将它禁用。那么该如何禁用 Windows 自带的 TFTP 客户端程序运行呢？通过下面的方面可以让 TFTP 客户端程序无法运行。

1. 测试正常的 TFTP 传输

先启动一个 TFTP 服务器，并放一个名为 snmp.zip 的程序作为测试之用。接着启动命令行 TFTP 客户端，下载 snmp.zip 程序。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在提示符后输入“tftp -i（对方 ip）get（文件名）”，如“tftp -i 192.168.0.4 get snmp.zip”，如图 9-21 所示。通过测试，文件可以顺利传输。



图 9-21

2．修改文件，禁止 TFTP 客户端运行

用文本编辑工具打开%systemroot%\system32\drivers\etc 下的 service 文件，找到对应的 tftp 那一行（如图 9-22 所示），将“69/udp”替换成“0/udp”，保存退出。

接着再尝试看看能否使用 TFTP，再次在提示符后输入“tftp -i 192.168.0.4 get snmp.zip”，按回车键，会提示“Timeout occurred”，已经无法从命令行下进行 TFTP 的文件传输了，如图 9-23 所示。



图 9-22

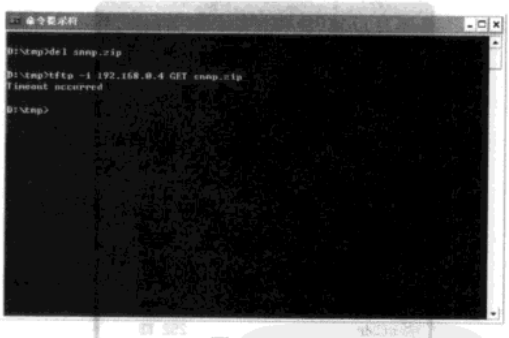


图 9-23

小知识 “%systemroot%”指系统安装目录。假设系统安装在 C 盘，对于 Windows 2000 系统是指 C:\WINNT；对于 Windows XP 是指 C:\WINDOWS。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第10章 超级启动盘应用经典案例

所谓超级启动盘就是在基本启动盘的基础上，通过集成大量实用的 DOS 工具、汉化工具、新设备的 DOS 版驱动程序、批处理程序，使得原本简单的启动盘拥有了强大的系统维护能力，而且使用更加简单、方便。

案例 105 引导计算机从 DOS 进入 Windows

一般情况下，只能通过启动盘进入纯 DOS 中，而不能在启动盘的引导下直接进入 Windows 系统中。那么要想从启动盘直接引导进入 Windows 系统，可以通过下面的方法实现。

将 Windows 98 系统下的 MSDOS.SYS 文件（如图 10-1 所示）拷贝到启动盘下，并替换同名文件，如图 10-2 所示。



图 10-1

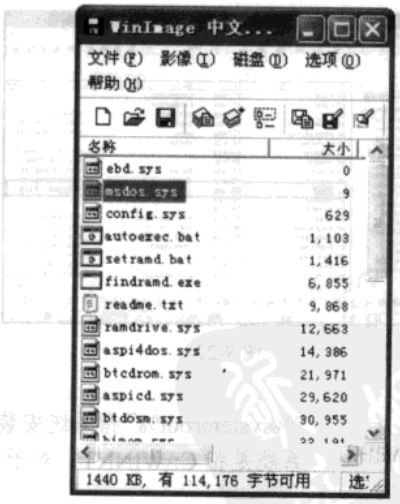


图 10-2

以后就可以用这张启动盘直接引导进入 Windows 系统。经测试，文件替换之后启动盘首先将系统引导到光驱启动菜单下，如图 10-3 所示；接着随意加载或不加载光驱，都能直接引导系统进入蓝天白云画面，如图 10-4 所示，从而顺利地进入正常的 Windows 98 桌面。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

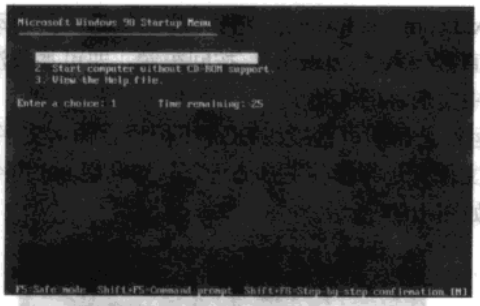


图 10-3



图 10-4

案例 106 让 DOS 支持 USB 设备

现在计算机周边应用中的 USB 设备越来越多了，而在 DOS 时代根本没有 USB 设备的概念，所以就谈不上支持 USB 设备。不过经过 DOS 爱好者的努力，终于开发出了可用于支持 USB 设备的程序 DUSE（下载地址：http://www.pocketec.net/downloads/ duse_4_4.zip）。

下载解压后，会看到 duse.exe 和 duseldr.com 这 2 个文件，将它们拷贝到启动盘中。利用启动盘进入到 DOS 下，在提示符后输入“duseldr a:\duse.exe”，按回车键，从而在 DOS 下加载 USB Stack Driver 驱动，即 USB 硬盘驱动，如图 10-5 所示。

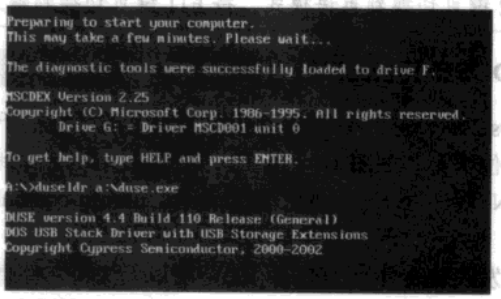


图 10-5

接下来，用户就可以在 DOS 下使用 USB 硬盘设备。若用户要加载的是 USB 光驱，除需加载 DUSE 驱动程序外，还需运行光驱扩展驱动程序，可以使用 DOS 自带的 mscdex.exe 程序。而 DUSE 的默认光驱设备名是 USBCDROM，所以在提示符后输入“mscdex.exe:mscdex /d:usbcdrom/”，按回车键，即可在 DOS 下加载光驱。

案例 107 让 DOS 也能支持中文名显示

在纯 DOS 下是无法显示中文文件名的，但是在 Windows 平台中为了方便记忆，一般都给文件和文件夹起了中文名称。要让纯 DOS 也能支持中文名显示，只需在启动时加载一个汉字系统就可以了。

在 DOS 下使用的汉字系统除 UCDOS、CCDOS97、AW97 外，还有一些 DOS 爱好者制作的更为小巧的 DOS 汉字系统，如 XZL 袖珍龙汉字系统（下载地址：http://crc.onlinedown.net82/down/xzl.zip）、天汇汉字系统等。下面以 XZL 袖珍龙汉字系统为例进行讲解。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

下载 XZL 且解压后，会看到 readme.exe、xzl.com、xzlpy.com 文件，将它们拷贝到启动盘中。利用启动盘进入到 DOS 下，在提示符后直接输入“xzl.com”，按回车键，即可加载汉字系统，如图 10-6 所示。加载后，就可以显示中文名称的文件夹。

其中的 xzlpy.com 是一个拼音输入法程序，运行之后即可直接在 DOS 下用拼音输入文字。通过这样的操作，使得在 DOS 下对中文名称的文件夹进行操作更加方便了，如利用 md 命令在 DOS 下创建中文名称的文件夹“新 DOS”，如图 10-7 所示。



图 10-6



图 10-7

注意 加载了 XZL 后，可运行 xzlpy.com，不过在 DOS 下只能一次输入 1 个汉字。另外，按 F12 键可切换到英语模式，按 F11 键可切换到输入法模式。

案例 108 让 DOS 支持长文件名

纯 DOS 与 Windows 2000/XP/2003 的命令提示符最大的区别在于，纯 DOS 不支持长文件名，最多只能显示前 6 位字符，如图 10-8 所示。要想在 DOS 下看到完整的文件名，可以在启动盘中加载 DOSLFN 程序（下载地址：http://www-user.tu-chemnitz.de/~heha/hs_freeware/doslfn.zip）。

下载并解压后，可发现该文件有 500 多 KB，所以无法将文件直接载入到启动盘中。用户可以将该工具放入硬盘的 FAT32 格式的盘符中，需要用时利用启动盘进入 DOS 下，然后进入该工具保存的目录下。在提示符后输入“DOSLFN.COM”，按回车键，开始加载。

加载后，DOS 就可以支持长文件名，这时在原磁盘目录后显示出了完整的文件名，如图 10-9 所示。

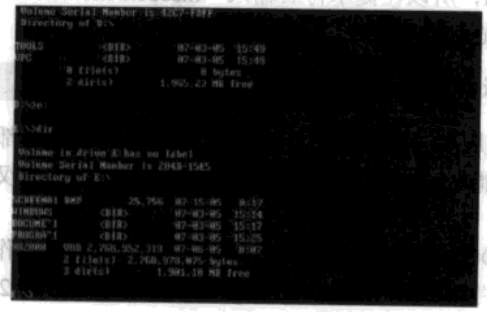


图 10-8



图 10-9

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

案例 109 让启动盘也能访问“网上邻居”

Norton Ghost 2003 中有一个实用的启动盘工具，通过该工具用户可以创建一个特殊的启动盘。利用该启动盘可以自由地访问局域网上的网上邻居，以便从网上邻居获得系统维护所需要的资源。

1. 制作可以访问“网上邻居”的启动盘

【第一步】在 Windows 系统中运行 Norton Ghost 2003，单击“Ghost 实用工具”，在展开的窗口右侧单击“Norton Ghost 启动向导”，进入“Norton Ghost 启动向导”窗口中，如图 10-10 所示。

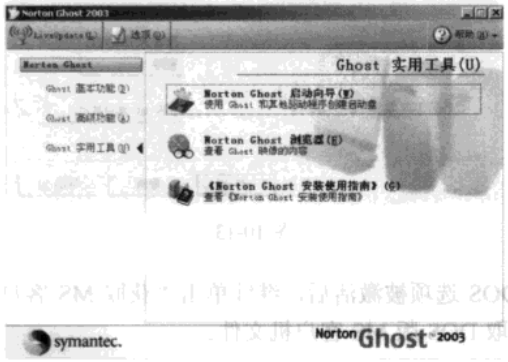


图 10-10

【第二步】在列表中选择“驱动器映射启动盘”选项，如图 10-11 所示。

【第三步】单击“下一步”按钮进入“Norton Ghost 启动向导 - 网络接口卡”窗口中。Ghost 2003 内置了常见网卡驱动，显示在下面的列表中，如图 10-12 所示。若网卡列表中有自己的网卡驱动，直接将其选中；若没有，可通过单击“添加”按钮，把网卡的驱动程序添加进来。

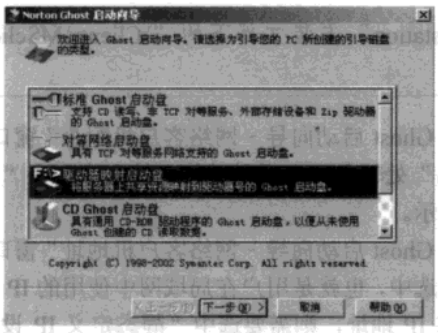


图 10-11

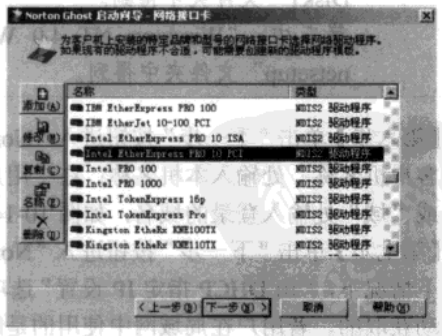


图 10-12

注意 选用的网卡驱动类型，必须是 NDIS2 的 DOS 版驱动，即支持 DOS 平台的网卡驱动程序。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

【第四步】网卡驱动选择好后，单击“下一步”按钮进入“Norton Ghost 启动向导 - DOS 版本”窗口中。在该窗口中选择启动盘中的 DOS 版本，是使用 PC-DOS，还是 MS-DOS。默认下只能选用 PC-DOS。对于用户普遍使用 MS-DOS，首先需要激活 MS-DOS 选项。要激活 MS-DOS 选项，先向软驱插入一张 MS-DOS 启动盘，接着单击“获得 MS-DOS”按钮，以获取启动文件，完成后“使用 MS-DOS”选项变为可用，如图 10-13 所示。

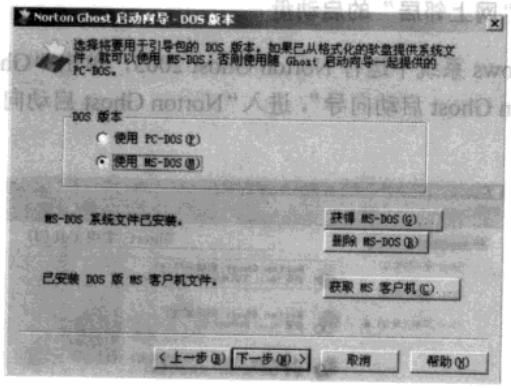


图 10-13

【第五步】当 MS-DOS 选项被激活后，继续单击“获取 MS 客户机”按钮，通过对弹出的对话框的操作，以获取 DOS 版 MS 客户机文件。

注意

单击“获取 MS 客户机”按钮，就是要向制作的启动盘中拷贝一些网络启动文件。所需的网络启动文件，可以 3 种方法得到。

第一种：用户可从 Microsoft Network Client 客户端安装程序中得到（下载地址：http://www.idp.net/freesoft/netclient.asp）。

第二种：从“Windows NT 4.0 Server”安装文件下的“\Clients\MSclient\Disks\Disk1”文件夹中得到。

第三中：“Windows NT 4.0 Workstation”安装文件下的“\Clients\MSclient\netsetup”文件夹中得到。

【第六步】单击“下一步”按钮进入“Norton Ghost 启动向导 - 网络客户机配查”窗口中，在“客户机名称”处输入本机名称；在“用户名”处输入本机登录网络时的名字；在“工作级”或“域”处输入登录的域名，如图 10-14 所示。

【第七步】单击“下一步”按钮进入“Norton Ghost 启动向导 - 网络客户机地址”窗口中。默认下情况下，“由 DHCP 指定 IP 设置”选项被选中，也就是用户在局域网中使用的 IP 地址是自动获取的。若用户在局域网中使用的是静态 IP 地址，则需要选中“静态定义 IP 设置”选项，然后在下面的“第一个 IP 地址”、“子网掩码”、“网关”、“DNS 地址”中，分别输入与本机相同的设置信息，如图 10-15 所示。

【第八步】单击“下一步”按钮进入“Norton Ghost 启动向导 - 目标驱动器”窗口中，根据向导提示将插入的启动盘取出，再插入 1 张空白软盘并进行格式化，如图 10-16 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

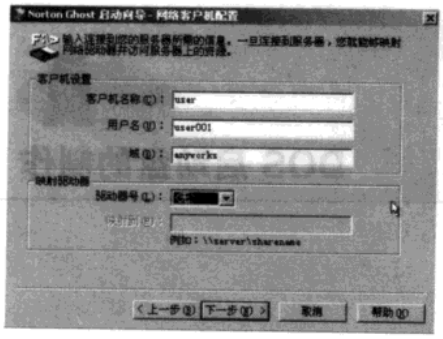


图 10-14

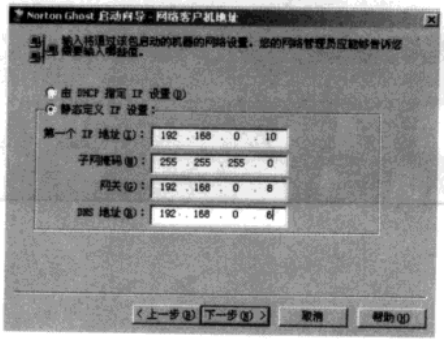


图 10-15

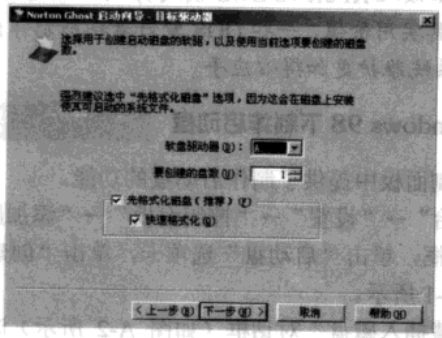


图 10-16

【第九步】单击“下一步”按钮开始对软盘进行格式化。格式化完成后，向导自动将网络启动盘必须的所有文件拷入软盘，以完成启动盘的制作。最后关闭制作向导即可。

2．利用制作的启动盘访问“网上邻居”中的资源

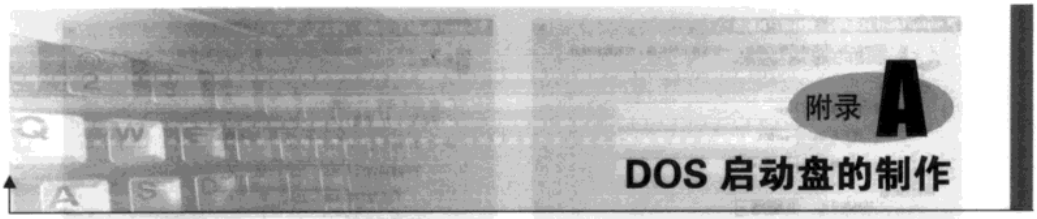
利用上面制作的启动盘可启动系统，不过在访问“网上邻居”时提示用户输入本机名、用户登录口令和所在域，这就是在制作启动盘时所输入的信息。正确输入后即可登录到网络上。

在提示符后输入“net view”，按回车键，将列出所有在同一工作组中的用户机器名。接着再次在提示符后输入“net view \\server01”，按回车键，即可查看 server01 服务器上的共享资源。

若在提示符后输入“net use Z: \\USER001\film”，按回车键，可将\\USER001 工作站中的 film 文件夹映射为本机的 Z 盘。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



附录 A DOS 启动盘的制作

启动盘是通往 DOS 的桥梁，对于仅安装了 Windows 2000/XP 操作系统的用户来说，如果不借助某些专业软件（如矮人 XP2K 纯 DOS 模式），则必须通过启动盘才能进入 DOS 进行系统维护。因为启动盘极具实用价值，一些 DOS 爱好者特别制作出集成了更多、更强大工具的启动盘，使 DOS 下的系统维护更加得心应手。

案例 110　在 Windows 98 下制作启动盘

在 Windows 98 的控制面板中提供了制作启动盘的功能。

【第一步】单击“开始”→“设置”→“控制面板”→“添加删除程序”选项，打开“添加/删除程序 属性”对话框，单击“启动盘”选项卡，单击“创建启动盘”按钮，启动创建启动盘系统程序，如图 A-1 所示。

【第二步】当弹出“请插入磁盘”对话框（如图 A-2 所示）时。按提示把准备好的软盘插入软驱。

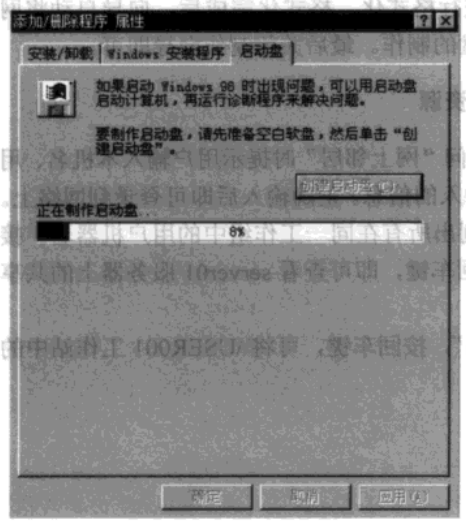


图 A-1

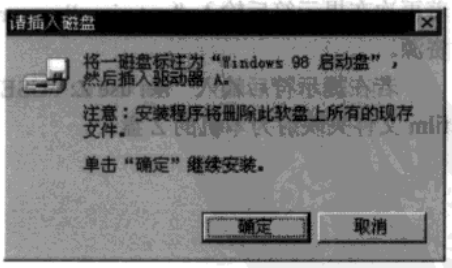


图 A-2

【第三步】确定之后，系统开始向软磁盘写入文件，如图 A-3 所示。当进度条抵达尽头时，启动盘即创建完毕。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

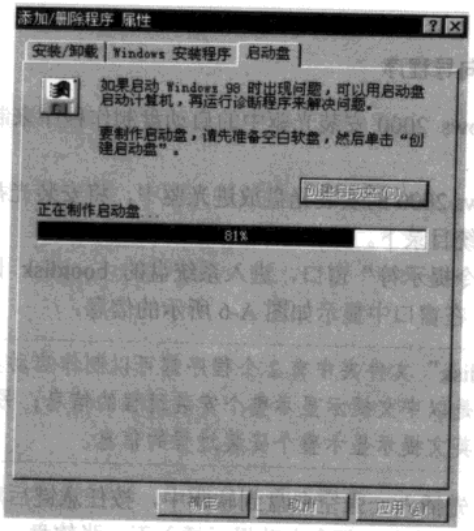


图 A-3

【第四步】取出软磁盘，存放于安全位置备用。

案例 111 在 DOS 下制作启动盘

当 Windows 98 系统崩溃无法进入，想重装系统但又没有启动盘时，可以考虑从 DOS 创建一张启动盘。当然，这需要系统至少还能进入 DOS 状态。具体的创建操作如下。

启动时按 F8 键显示启动菜单，选择 Command Prompt Only 方式进入 DOS 下，进入 C:\WINDOWS\command 目录，如图 A-4 所示。运行 bootdisk.bat 批处理文件，如图 A-5 所示。

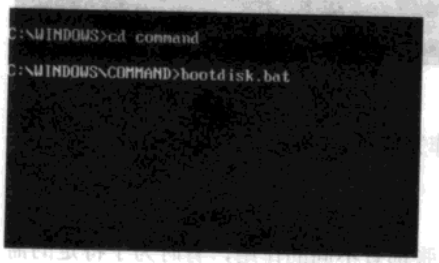


图 A-4

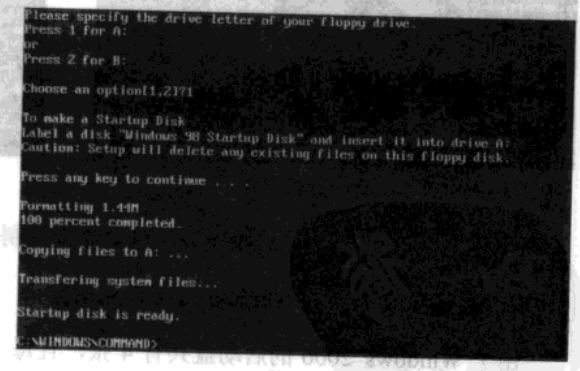


图 A-5

运行后首先提示选择驱动器 A 还是 B，选择 A（按 1 数字键），插入一张已格式化的软盘并按回车键。稍等片刻，启动盘创建完毕。

案例 112 制作 Windows 2000 启动盘

虽然 Windows 2000 系统没有提供制作启动盘功能，但也可以使用以下两种方法来制作

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

启动盘。

1．利用启动盘制作向导程序

此方法是利用 Windows 2000 安装光驱中的启动盘制作程序来制作启动盘，具体的操作如下。

【第一步】把 Windows 2000 的安装光盘放进光驱中，将安装光盘中的 bootdisk 文件夹复制到 Windows 2000 的系统目录下。

【第二步】打开“命令提示符”窗口，进入系统盘的 bootdisk 目录下，在提示符后输入“makebt32”，按回车键，在窗口中显示如图 A-6 所示的信息。

小提示 在“bootdisk”文件夹中有 2 个程序都可以制作启动盘，一个是 makebt32 程序，特点是以中文提示显示整个安装过程的信息；另一个是 makeboot 程序，特点是以英文提示显示整个安装过程的信息。

【第三步】提示用户先插入一张空白盘到软驱中，按任意键后对软盘进行格式化，并复制启动文件。每做好一张启动盘，都会自动提示插入下一张软盘。直到 4 张启动盘全部作好为止，如图 A-7 所示。而且系统依次为每张制作的启动盘进行编号，如 Windows 2000 Setup Boot Disk #1、Windows 2000 Setup Boot Disk #2、Windows 2000 Setup Boot Disk #3、Windows 2000 Setup Boot Disk #4。

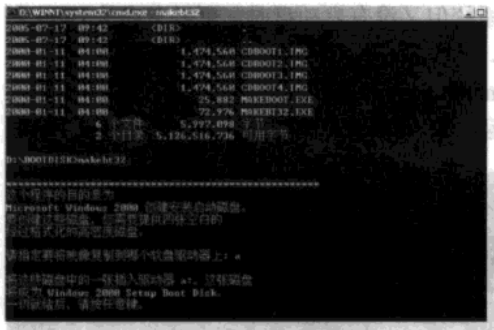


图 A-6



图 A-7

【第四步】完成了上面的操作后，启动盘也就制作完成了。

2．直接释放法制作 Windows 2000 启动盘

由于 Windows 2000 的启动盘共有 4 张，且每一张都有不同的作用，有时为了特定的需要，用户可能只需要用到其中一张启动盘。但是如果按照上面方法运行 makebt32 或 makeboot 程序，就只能从第一张启动盘开始制作。

其实，在系统的 bootdisk 文件夹下面包含了 cdboot1.img、cdboot2.img、cdboot3.img、cdboot4.img 这 4 个文件，它们分别对应着 Windows 2000 的 4 张启动盘中的内容。用户需要制作指定启动盘时，只要找到对应的 IMG 格式文件，然后使用专门的释放工具，将内容释放到软盘中就可以了。这里以 UNIMG 工具为例介绍制作 2#启动盘的操作方法。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

首先用户必须将 bootdisk 文件夹及 UNIMG 工具复制到 Windows 2000 的安装目录下，同时确保 UNIMG 运行程序和 cdboot2.img 文件在同一文件夹下。

重新启动计算机，让系统进入 DOS 提示符状态，并进入到 BootDisk 文件夹下，然后在命令行状态下输入“unimg cdboot2.img”，按回车键。接着再用 dir 命令查看一下 bootdisk 文件夹，可以发现多出了 cdboot2 这个文件夹，在这个文件夹中就放置了 Windows 2000 2#启动盘中的内容。

最后将 cdboot2 这个文件夹中的所有内容复制到格式化好的软盘中，Windows 2000 2#启动盘就算制作成功了。如果还需要制作其他的启动盘，可以按照上面的方法，释放对应的 IMG 格式文件，并把释放后的文件直接复制到软盘中就可以了。

案例 113 制作 Windows XP 启动盘

Windows XP 启动盘制作的方法与 Windows 2000 相似，不过制作程序没有集成在 Windows XP 安装光盘中，如果需要可从微软公司的网站下载，或到一些专业下载站点下载。

微软公司网站的下载地址如下。

http://www.microsoft.com/downloads/info.aspx?na=90&p=&SrcDisplayLang=zh-cn&SrcCategoryId=&SrcFamilyId=55820EDB-5039-4955-BCB7-4FED408EA73F&u=http%3a%2f%2fdownload.microsoft.com%2fdownload%2fwhistler%2fInstall%2f310994%2fWIN98MeXP%2fCN%2fWinXP_CN_PRO_BF.exe

太平洋下载页面的地址如下。

http://dl.pcgames.com.cn/html/1/5/dlid=5825&dltypeid=1&pn=0&linkPage=1.html

启动盘制作工具是一个自解压文件，直接运行打开命令提示符窗口，按提示输入，然后依次插入 1～6 张准备好的空白格式化的软盘，即可完成启动盘的制作。如图 A-8 所示。

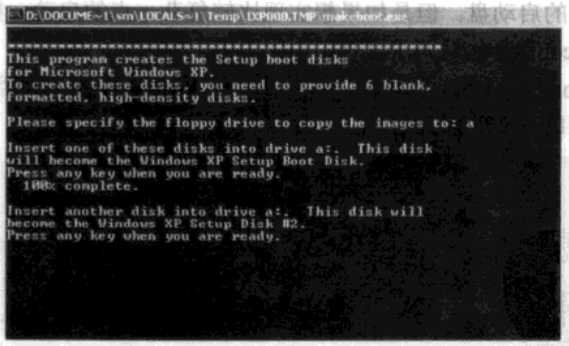


图 A-8

案例 114 制作 Windows XP 密码破解启动盘

在 Windows XP 中提供了一个制作密码启动盘的工具，它可以“破解”Windows XP 系统中所有的账户密码。

打开“控制面板”→“用户账户”，在“用户账户”窗口单击自己的账户，进入账户设置页面，单击左上方的“阻止一个已忘记的密码”选项，如图 A-9 所示，打开“忘记密码向导”。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 A-9

将一张格式化过的空白磁盘插入到软驱中，按照“忘记密码向导”提示单击“下一步”按钮，中间会要求输入这个账户现在的密码，输入后等待几秒钟即可创建完成密码启动盘。

以后，如果在系统启动的时候忘了密码，只要单击账户旁边向右的箭头，然后在弹出的提示栏中点击“使用密码重设磁盘”，再将软盘插入软驱，即可按照提示更改密码并启动计算机。

案例 115　制作 USB 启动盘

要制作 USB 启动盘，需先要下载 USBoot 这个小程序（下载地址：http://nj.onlinedown.net/soft/34696.htm）。

该程序自带了 MS-DOS 7.10 的两个基本启动文件 IO.SYS 和 COMMAND.COM，可将 U 盘格式化为一个基本的启动盘。但是如果想实现比较复杂一点的启动，如加载光驱，则还要编辑 autoexec.bat 和 config.sys 这两个文件。

首先，用 USBoot 制作 USB 启动盘，然后找一张 Windows 98 启动盘或下载 Windows 98 启动盘影像文件，把以下文件拷入 U 盘。

```
autoexec.bat
config.sys
emm386.exe
smartdrv.exe
edit.com
format.com
fdisk.exe
himem.sys
mscdex.exe
oakcdrom.sys
```

接着，编辑 autoexec.bat 文件，即加入以下指令（可以用 edit 工具编辑）。

```
@echo off
LH a:\\mscdex.exe /d:mscd001
LH a:\\smartdrv.exe
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

再接着，编辑 config.sys 文件，加入以下指令：

```
device=a:\\himem.sys
device=a:\\emm386.noems
device=a:\\oakcdrom.sys /D:mscd001
dos=high,umb
files=40
buffers=30,0
stacks=9,256
lastdrivers=z
```

以上操作完成后，所制作的 USB 启动盘即可实现加载光驱和磁盘缓存启动系统了。

案例 116　制作硬盘版 DOS 启动

除了可以制作软盘启动盘、U 盘启动盘等，还可以直接在硬盘中制作硬盘版 DOS 启动。这对于使用 Windows 2000/XP/2003 系统的用户，是直接进入纯 DOS 中的最佳启动方案。如要实现这个功能，可以利用以下的方法。

1. 向 Windows 2000/XP/2003 系统盘传送能进入纯 DOS 下的启动文件

在新装系统（Windows 2000/XP/2003）之前，如果 C 盘是 FAT32 格式，那么可以用 Windows 98 的 DOS 启动盘启动系统。

接着，在提示符后输入“sys c:”，按回车键，向 C 盘传递 DOS 的 3 个基本启动文件。

然后，在安装 Windows 2000/XP/2003 时，不要改变 C 盘的分区格式。Windows 安装完毕，再开机就会出现两个启动选项，如图 A-10 所示。其中“Microsoft Windows”就是 DOS 启动项。

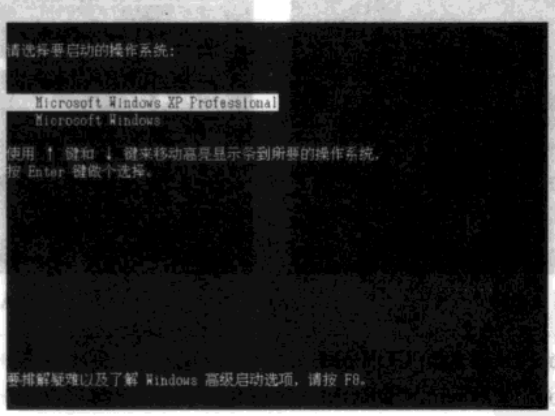


图 A-10

2. 利用第三方 DOS 虚拟工具来实现

此方法不适用单独的 Windows 98 系统，只适用于 Windows 2000/XP/2003 与 Windows 98 混合的多系统。也不必考虑 C 盘是 FAT32 格式，还是 NTFS 格式。只需要从网上下载 vFloopy 工具（下载地址：http://nj.onlinedown.net/soft/20055.htm），接着完成以下操作。

软件下载解压后，可以直接运行，弹出图 A-11 所示的窗口。接着单击“映像文件”栏

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

后面的选择映像文件路径按钮。在打开的对话框中选择工具自带的两个映像文件之一的 NTFS.img 文件，如图 A-12 所示。

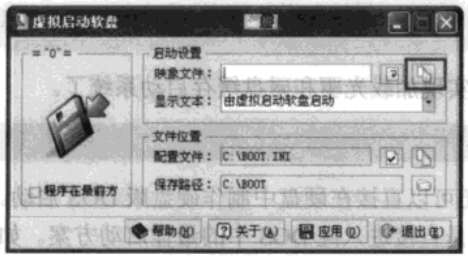


图 A-11



图 A-12

单击“打开”按钮，返回到图 11 所示的窗口中。使用默认值，单击“应用”按钮后，重新启动系统。系统启动后在启动菜单中会多出“由虚拟启动软盘启动”选项，如图 A-13 所示，这就是用虚拟 DOS 工具制作的启动项。选中它并按回车键，就会进入图 A-14 所示的 DOS 启动菜单界面下。

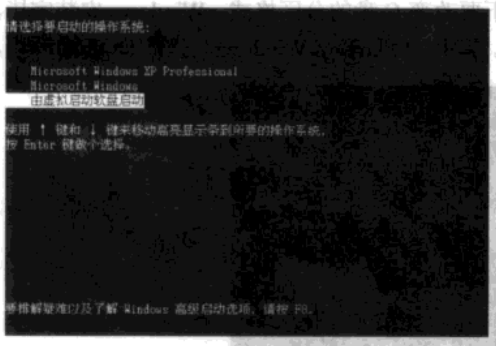


图 A-13



图 A-14

认识 DOS 启动菜单的含意

Boot DOS with CDROM	标准功能+光驱驱动
Boot DOS with CDROM + NTFS	标准功能+光驱驱动+读写 NTFS 分区
Boot DOS with CDROM + U-DISK	标准功能+光驱驱动+U 盘驱动
Boot DOS with CDROM + U-DISK + NTFS	标准功能+光驱驱动+U 盘驱动+读写 NTFS 分区
Boot DOS ONLY (No Any Driver).	只启动基本 DOS 系统
REBOOT YOUR PC.	重启计算机
SHUTDOWN YOUR PC.	关闭计算机

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

用户可以选择需要的启动方式，按回车键确定。启动成功后，会显示“DOS LOADING SUCCESSFUL”的字样，并定位到 A:\>提示符下，如图 A-15 所示。

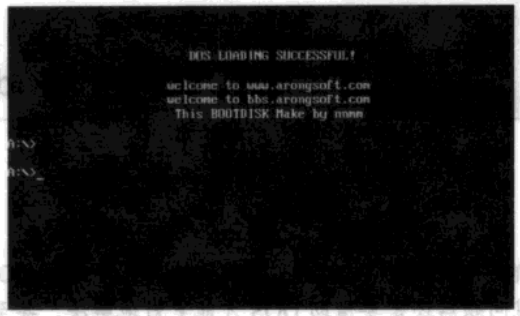
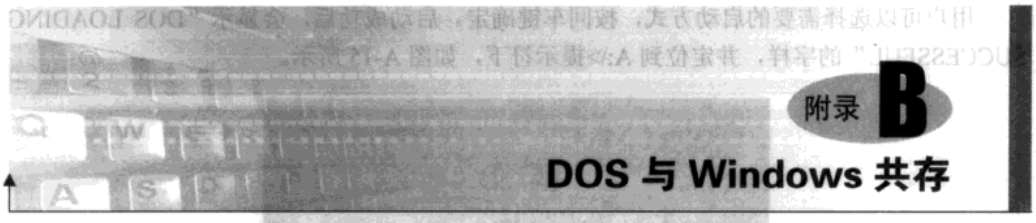


图 A-15

至此，硬盘版的 DOS 启动已经制作成功，只要用户不重装系统或格式化系统盘，这个 DOS 引导菜单就会一直存在。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



附录 B DOS 与 Windows 共存

现在大家使用的都是可视化的 Windows 操作系统，也许早把 DOS 系统抛之脑后。事实上，Windows 系统出现问题后还是要借助 DOS 才能更好地解决，甚至有些问题不在 DOS 下是无法解决的。而表面上看，已经屏蔽了 DOS（实模式）的 Windows 2000/XP/2003 系统，其内部反而集成了更多的 DOS 命令（保护模式），这也正说明了 DOS 的重要性。

如果使用的是 Windows 2000/XP/2003 系统，要想进入纯 DOS 平台，就不像 Windows 98 那么方便。很多用户都使用双系统或多系统共存，其实完全可以让纯 DOS 也成为它们其中一员。

案例 117　使用第三方工具来实现纯 DOS 与 Windows 系统共存

如果让电脑初学者在一分钟内实现让 Windows 2000/XP/2003 与 DOS 共存，是不是不可思议？从网上可以下载一个非常优秀的 DOS 启动菜单制作工具——vFloppy，只需要进行简单的设置操作，就可以在启动菜单中创建一个纯 DOS 启动菜单项。当用户启动系统时，进入启动菜单中选择该启动菜单，就可以直接进入纯 DOS 下。下面来看看具体的创建过程。

vFloppy 工具可以从华军软件园、天空软件站等各大的主流下载网站中下载，下载后进行解压。解压后，运行 vFloppy.exe 文件，打开“vFloppy”界面，如图 B-1 所示。

单击“映像文件”栏右边的“打开”按钮，在弹出的窗口中选中“BootDisk.img”文件，如图 B-2 所示。



图 B-1



图 B-2

单击“打开”按钮，在“显示文本”中用户可以随意将“由虚拟启动软盘启动”改为用户想定义的文字信息（此处的文字信息就是启动菜单中所显示的文字），如改为“虚拟 DOS 启动盘”，如图 B-3 所示。设置完成后，单击“应用”按钮弹出“执行结果”窗口，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如图 B-4 所示。

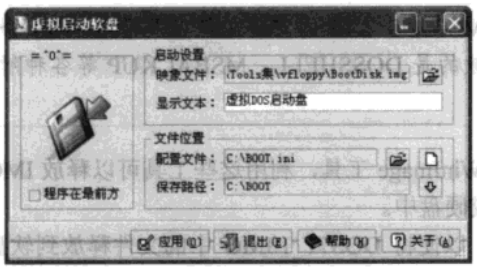


图 B-3

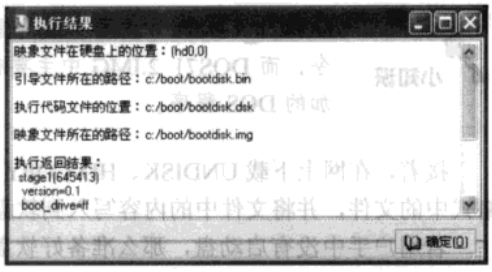


图 B-4

单击“确定”按钮就可以将窗口中显示的三个文件拷贝到 Boot 文件夹中，并需要重新启动计算机。重启后会在启动菜单中看到所创建的“虚拟 DOS 启动盘”选项，如图 B-5 所示。

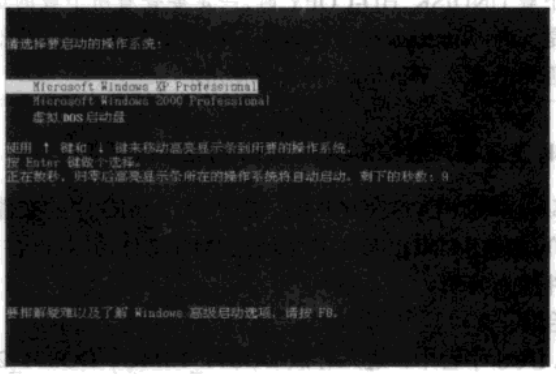


图 B-5

以后要进入纯 DOS 下，只需要在启动菜单中选中“虚拟 DOS 启动盘”选项，即可进入纯 DOS 下，而不需要使用启动盘。

案例 118　安装 MS-DOS 7.10 来实现纯 DOS 与 Windows 系统共存

MS-DOS 6.22 是现在使用最为普遍的 MS-DOS 版本，Windows 98 中也自带了该版本，利用它足以解决各类硬盘、系统所出现的故障和问题，但是它不支持大硬盘、大内存、长文件名（LFN）等功能。而最新的 MS-DOS 7.10 是目前功能最为强大、兼容性最好的 MS-DOS 版本，它支持 MS-DOS 6.22 所不能支持的功能。而且安装 MS-DOS 7.10 后，会自动在启动菜单中生成启动项，利用该启动项用户可以直接进入 MS-DOS 7.10 中，从而实现 DOS 与 Windows 共存。

1．安装 MS-DOS 7.10 前的准备工作

要顺利地安装 MS-DOS 7.10，需要做以下的准备工作。

首先，要从网上下载 MS-DOS 7.10 的安装程序，可以从华军软件园、天空软件站等主流下载网站中下载。下载解压后，文件夹中有两个 IMG 文件，分别是 DOS71_1.IMG、

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

DOS71_2.IMG，这 2 个文件就是 MS-DOS 7.10 的安装文件。

小知识 DOS71_1.IMG 中主要存放的是 MS-DOS 7.10 的安装文件以及常用 DOS 命令，而 DOS71_2.IMG 中主要存放的是 DOSSHELL、MSBACKUP 等各种附加的 DOS 程序。

接着，在网上下载 UNDISK、HD-COPY、WinImage 工具，利用这些工具可以释放 IMG 格式中的文件，并将文件中的内容写入到软盘或硬盘中。

若用户手中没有启动盘，那么准备好软盘。以便将 DOS71_1.IMG 中的文件释放到软盘中，释放后便是一张启动盘和 MS-DOS 7.10 安装盘。

最后，将 DOS71_1.IMG、DOS71_2.IMG、UNDISK、HD-COPY、WinImage 文件放入 FAT32 格式的盘符中，以便在 DOS 下可以识别。

注意 用户在下载 UNDISK、HD-COPY 时，一定要查看所下载的这款工具是支持 DOS 平台还是支持 Windows 平台。如果下载的是 DOS 版，那么只能在 DOS 平台中使用；否则只能在 Windows 平台中使用。

2. 使用 UNDISK 工具来释放 MS-DOS 7.10 到软件或硬盘中

以上 3 款工具都可以释放 DOS71_1.IMG、DOS71_2.IMG 中的文件到软盘或硬盘中，因篇幅的关系，这里只介绍使用 UNDISK 工具来释放 IMG 文件，并且以在 DOS 平台和 Windows 平台中释放 IMG 文件操作为例。

（1）在 DOS 平台中

利用启动盘进入 DOS 平台中，进入存放 DOS71_1.IMG、DOS71_2.IMG、UNDISK 的盘符目录中，如图 B-6 所示。接着在命令提示符后输入“undisk dos71_1.img”，按回车键，这时会弹出如图 B-7 所示的信息。

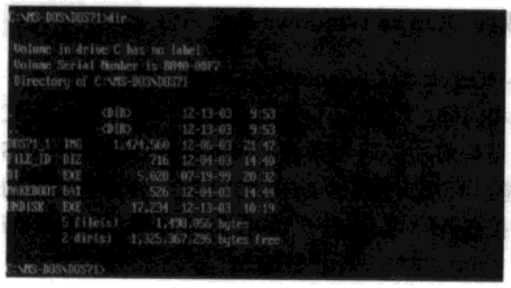


图 B-6

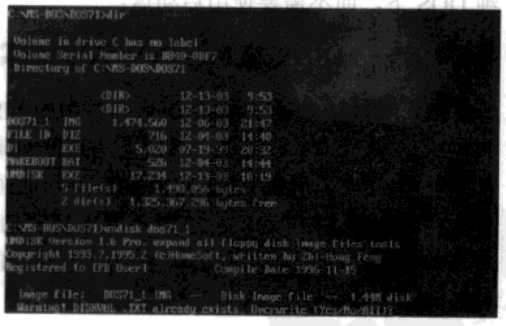


图 B-7

要释放 MS-DOS 7.10 安装文件，直接键输入“y”，按回车键，开始进行释放，并自动生成一个“DOS71_1”目录，如图 B-8 所示。此目录中就是 MS-DOS 7.10 所需要的安装文件。

再利用同样的方法来释放 DOS71_2.IMG 中的文件，并也自动生成一个“DOS71_2”目录。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

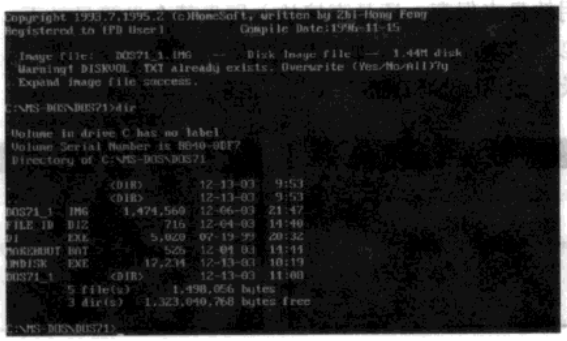


图 B-8

（2）在 Windows 平台中

在 Windows 平台中使用的 UNDISK 版本名为 UNDISKER，下载安装后运行程序进入主界面中，如图 B-9 所示。接着单击“File”→“Open”选项，在打开的对话框中先选中“DOS71_1.IMG”，如图 B-10 所示。



图 B-9

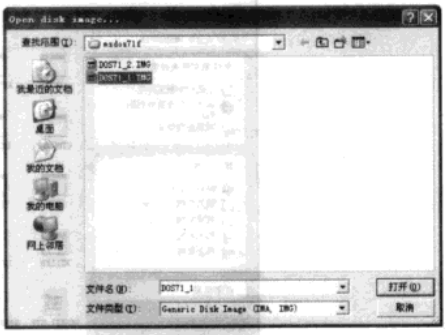


图 B-10

UNDISKER 开始自动对 DOS71_1.IMG 中的文件进行释放，释放后显示在文件列表中，如图 B-11 所示，这些文件就是 MS-DOS 7.10 所需要的安装文件。下面就可以对释放的文件进行保存，单击“Image”→“Extract To…”选项，如图 B-12 所示。

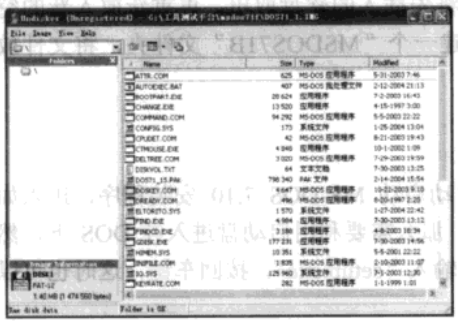


图 B-11



图 B-12

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

接下来选择是用软盘来保存，还是直接放入硬盘某个盘符目录下。若保存到软盘中，在“Extract To…”中可以直接输入“A:\”，如图 B-13 所示；若保存到硬盘中，可以单击“Browse…”按钮来选择保存目录，如“G:\MSDOS71A\”，如图 B-14 所示。

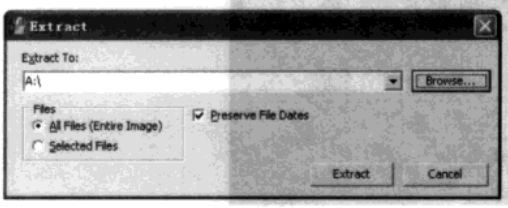


图 B-13

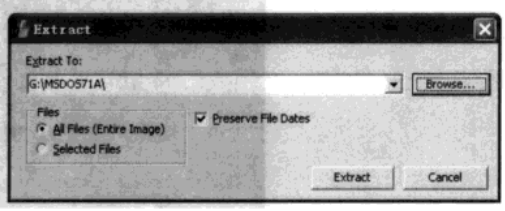


图 B-14

若保存到软盘中，这时就需要把准备好的空白软盘插入到软驱中，单击“Extract”按钮即可开始将释放的文件写入软盘中；若保存到硬盘上，在选择保存位置后直接单击“Extract”按钮即可将释放的文件写入保存目录中，如图 B-15 所示。

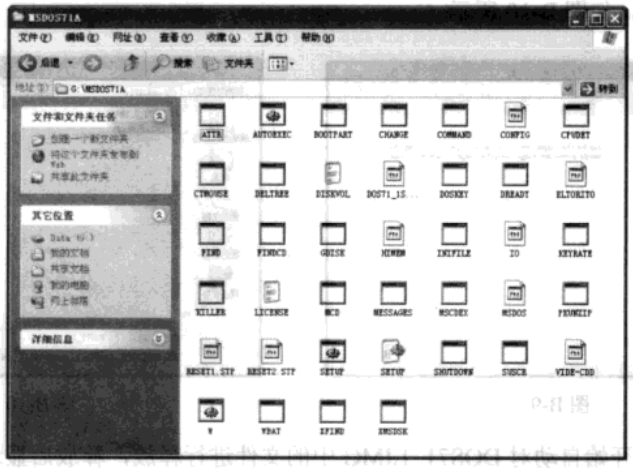


图 B-15

再利用同样的方法来释放 DOS71_2.IMG 中的文件，保存到软盘或硬盘目录中。在释放 DOS71_2.IMG 中的文件到软盘时，一定要记住将先插入的软盘取出，再重新放入新的空白软盘；而保存到硬盘目录中，最好在 G 盘中新建一个“MSDOS71B”文件夹，将文件放入其中。

3. MS-DOS 7.10 安装过程全图解析

接下来可以使用第一张软盘启动系统，会自动启动 MS-DOS 7.10 安装程序，进入如图 B-16 所示的安装界面中。如果是保存在硬盘中，那么需要利用启动盘进入纯 DOS 下，然后进入“DOS71_1”目录中，直接在命令提示符后输入“setup.exe”，按回车键，这时也可以进入“MS-DOS 7.10”安装界面。

在 MS-DOS 7.10 的安装界面中，先选择“Next”并按回车间进入如图 B-17 所示的界面。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

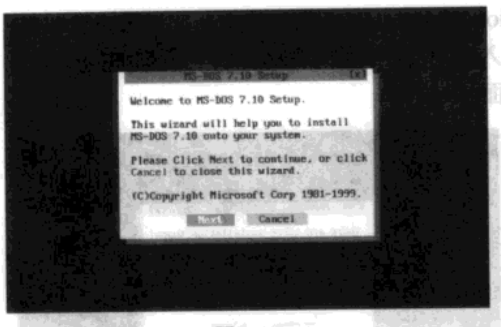


图 B-16

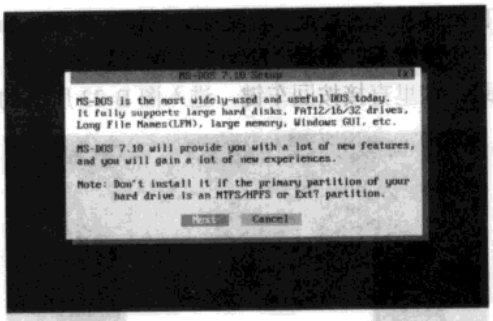


图 B-17

如果读者的英语水平比较高，可以看看上面的信息；如果欠缺，您也不必担心，只需要根据安装向导完成操作即可。此界面中的信息表示安装 MS-DOS 7.10 后可以支持 NTFS/HPFS 文件系统。这里用户可以直接按回车键进入如图 B-18 所示界面中。询问用户是否同意安装 MS-DOS 7.10，选择“I agree”按回车键，表示安装 MS-DOS 7.10，进入如图 B-19 所示的界面中；而选择“I don't agree”按回车，表示不安装 MS-DOS 7.10，并退出安装向导。

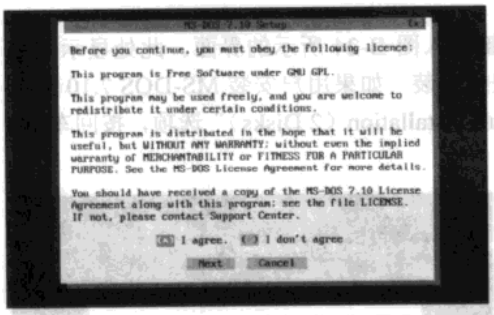


图 B-18

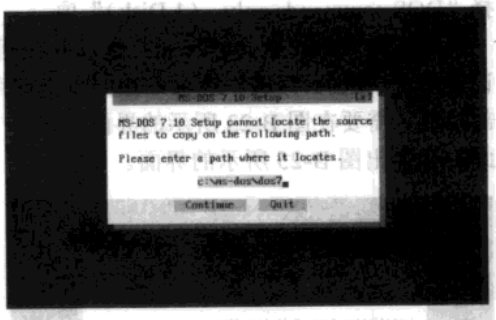


图 B-19

在如图 B-19 所示的安装界面中输入安装文件所在的地址，然后选择“Continue”项按回车键，进入如图 B-20 所示的界面，提示是否重写主引导记录。若重写，选择“YES”选项（推荐）按回车键进入如图 B-21 所示的界面；反之选择“No”选项。

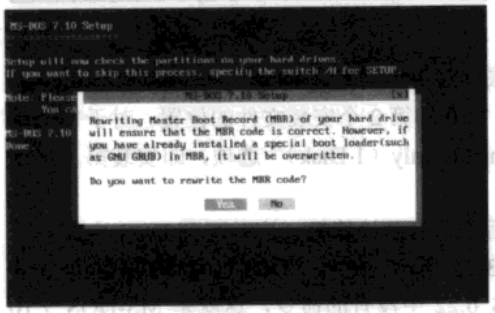


图 B-20

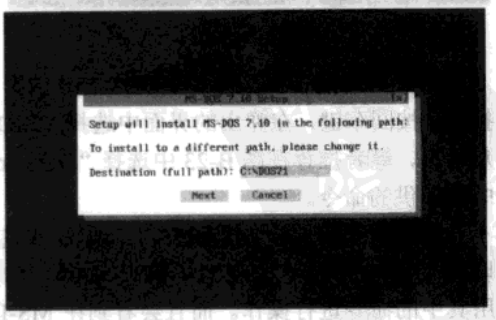


图 B-21

在图 B-21 中，主要是创建 MS-DOS 7.10 安装后的目录，系统默认值是 C:\DOS71，也可以

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

自己设置安装目录。若要重新设置，在“Destination（full path）:”框中输入新的目录路径即可。

设置后，选择“Next”选项并按回车键，进入图 B-22 所示的界面，确定所创建的安装目录。这里直接按回车键，进入图 B-23 所示的界面。

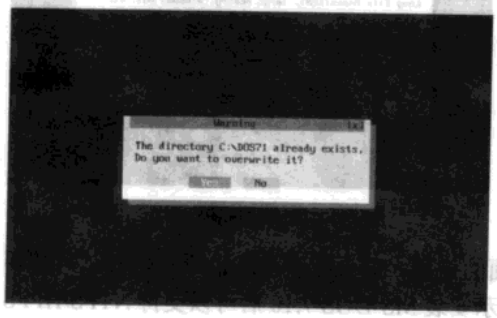


图 B-22

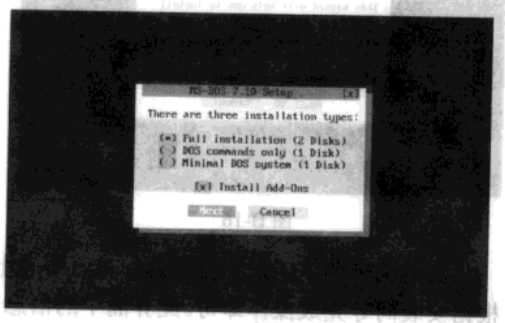


图 B-23

在图 B-23 中，可以有选择地安装 MS-DOS 7.10 的功能（在一开始安装 MS-DOS 7.10 时有两个文件，而后者是可选择的）。默认情况下是安装 MS-DOS 7.10 的全部功能，也可以选择“DOS commands only （1 Disk）”项。

设置完成后，选择“Next”选项并按回车键进入图 B-24 所示的界面。此处显示安装设置信息，选择“OK”选项后按回车键即可进行安装。如果用户安装 MS-DOS 7.10 的全部功能，需要在图 B-23 所示的界面中选择“Full installation（2 Disks）”选项，按回车键，此时会弹出图 B-25 所示的界面。

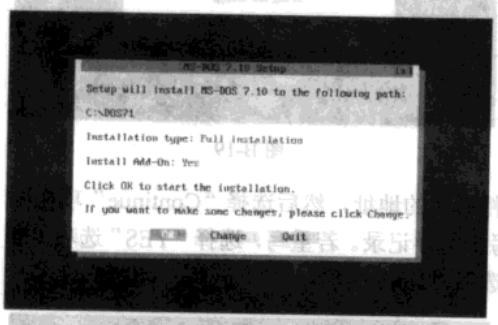


图 B-24

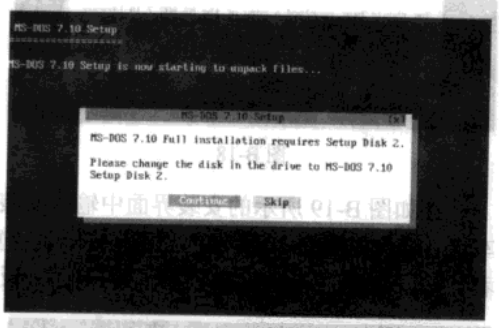


图 B-25

这时要求插入或选择 MS-DOS 7.10 的第 2 张安装盘（也就是 DISK 2），选中“Continue”按钮，按回车键，在弹出的界面中选择 MS-DOS 7.10 的第 2 个安装文件的位置。对于普通用户而言，笔者推荐在图 B-23 中选择“DOS commands only（1 Disk）”选项，即安装第 1 张盘中所提供的命令。

接下来开始安装 MS-DOS 7.10，安装完成后重新启动计算机。这时回到 DOS 中，就可以在 C 盘中看到创建的“DOS71”目录，如图 B-26 所示。进入“DOS71”目录中，可以使用其中的命令进行操作。而且会看到在 MS-DOS 6.22 中没有的命令，这就是 MS-DOS 7.10 的完美之处。

当 MS-DOS 7.10 安装完成后，则会在操作系统启动菜单中生成一个菜单选择项，如图

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

B-27 所示。



图 B-26

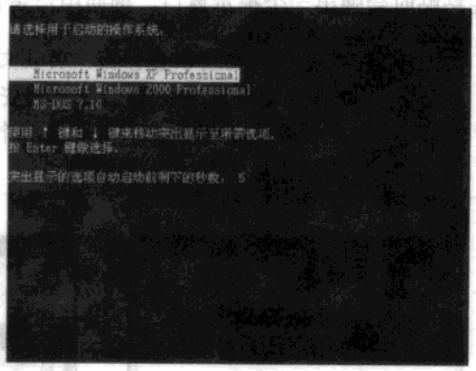


图 B-27

对于没有 Windows 98 的多操作系统，MS-DOS 7.10 是最理想的纯 DOS 平台了。利用它不仅可以直接进入纯 DOS 平台中，而且，此纯 DOS 的功能也比 Windows 98 自带的 MS-DOS 6.22 强大得多。当选择 MS-DOS 7.10 菜单选项后，就可以进入“MS-DOS 7.10”平台，如图 B-28 所示。

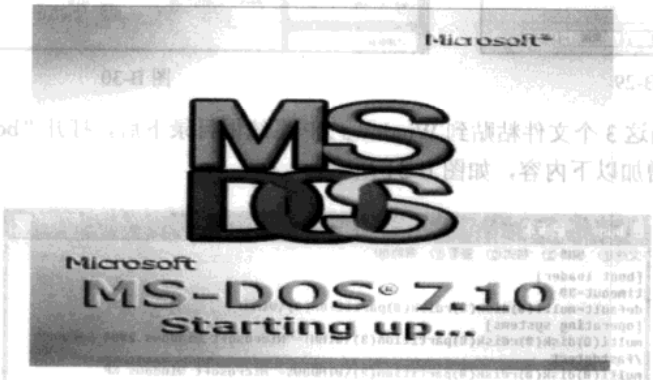


图 B-28

案例 119　手动设置实现纯 DOS 与 Windows 系统共存

除了使用软件来实现 Windows 2000/XP/2003 与纯 DOS 共存外，还可以通过手动制作的方法来达到这一目的。下面以 Windows XP 系统为例，介绍具体的设置方法。

【第一步】找一个有 Windows 98 系统的计算机，进入系统盘根目录下，找到 IO.SYS、MSDOS.SYS 和 COMMAND.COM 这 3 个文件。

注意　若要查看到这 3 个文件，必须进行以下操作：在“我的电脑”窗口中，单击“工具”→“文件夹选项”→“查看”选项卡，在“高级设置”栏中的将“隐藏受保护的操作系统文件”选项取消。再将“隐藏文件和文件夹”下的“显示所有文件和文件夹”选项选中，如图 B-29 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

【第二步】将这 3 个文件拷贝到软盘中，然后粘贴到自己的 Windows XP 系统根目录下。在粘贴时会弹出一个提示窗口，询问用户是否替换原有文件，单击“全部”按钮即可。

注意 在粘贴时之所以会弹出“确认文件替换”，主要是由 IO.SYS 和 MSDOS.SYS 这 2 个文件引起的。它们是系统安装的引导文件，在安装 Windows XP 系统后都会在系统盘根目录中生成这 2 个文件。但是，生成的这 2 个文件都是“0 字节”的空文件，如图 B-30 所示。

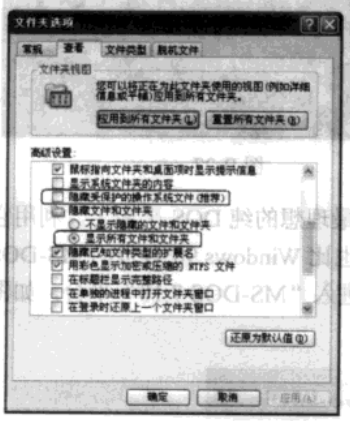


图 B-29

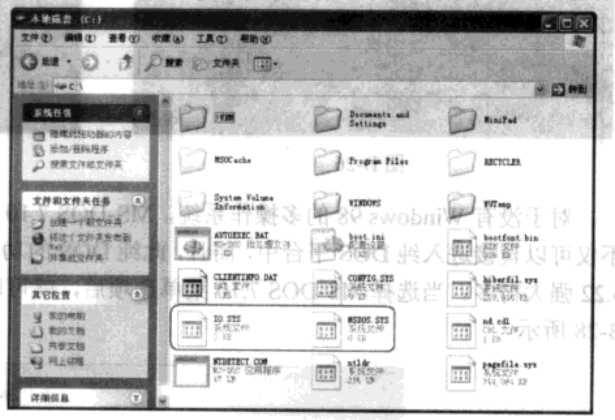


图 B-30

【第三步】当这 3 个文件粘贴到 Windows XP 系统根目录下后，打开“boot.ini”文件，在“boot.ini”文件增加以下内容，如图 B-31 所示。

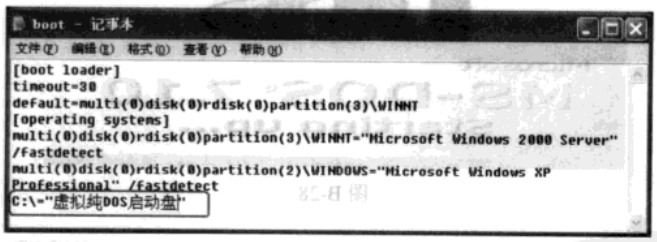


图 B-31

注意 这 3 个文件的大小分别是：IO.SYS 为 219KB、MSDOS.SYS 为 1～2KB、COMMAND.COM 为 93KB。如果大小不同，那么就需要关注一下，查看其是否感染病毒了。

【第四步】设置完成后，保存设置。重新启动计算机，这时就可以在启动菜单中看到“虚拟纯 DOS 启动盘”选项，选择此选项就可以直接进入纯 DOS。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

附录 C

最新流行DOS工具软件应用指南

正所谓“英雄所见略同”，一些软件开发人员也看到了DOS的实用价值。他们通过制作启动盘的方式把这些工具集成到一起，并精心编辑了一些批处理文件，使在DOS下的系统维护工作变得得心应手了。其中很多工具的功能值得读者动手实践。

案例120 矮人XP2K纯DOS模式2.0

“矮人XP2K纯DOS模式”是为仅安装了Windows 2000或XP的用户设计、帮助启动到DOS下进行系统维护的工具，它能够为Windows 2000/XP启动菜单加入纯DOS模式和备份恢复选项。不过它对Windows 98＋Windows 2000/XP的多操作系统不适用，会发生启动错误。但是在安装了Windows 98的多系统启动到DOS下已经不是问题（按F8键，选择Command Prompt Only），所以这个缺陷的影响不大。

该软件的主要功能，一是“矮人工作室纯DOS模式”，二是“矮人工作室备份恢复”。

1．矮人工作室纯DOS模式

“矮人工作室纯DOS模式”有5项选项，还有很多实用工具如KV3000杀毒等。它可以实现如下功能。

- 分区、格式化。
- 加载光驱。
- 加载缓存。
- 支持鼠标、NTFS。
- 加载中文支持，附带汉化的输入法。

首先要到网上下载该工具（下载页面：http://nj.onlinedown.net/soft/24990.htm）。接着在Windows 2000/XP系统中直接安装，安装完毕后重新启动系统，即可看见启动选项新增的两项，如图C-1所示。

选择“矮人工作室纯DOS模式”进入图C-2所示的引导菜单。

菜单中有三种光驱支持模式，即加载缓存、加载高端内存、支持中文。选择任意一项，都会加载光驱进入纯DOS模式的A盘下，然后就可以借助这个虚拟A盘的各种工具对系统进行维护操作了。

2．矮人工作室备份恢复

在启动菜单选择“矮人工作室备份恢复”也可以将系统引导到纯DOS下，并且启动另

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

一个著名的 DOS 下的系统备份工具“PowerWuest Drive Image Pro 4.0”，其功能和易用性不亚于 Ghost。

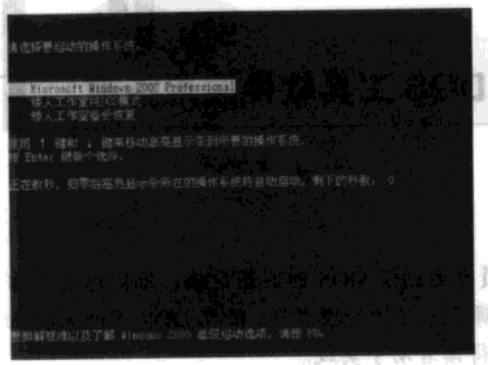


图 C-1

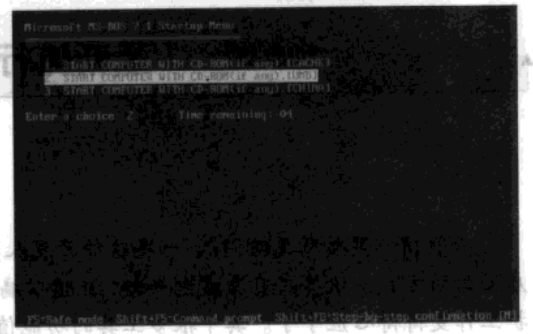


图 C-2

PowerWuest Drive Image Pro 主要用于创建整个系统分区的备份或从备份恢复系统分区。由于启动过程中已经加载了鼠标，所以在备份过程中可直接使用鼠标操作。

单击“创建映象”按钮启动向导，如图 C-3 所示。选中系统所在分区，这里选中了 Windows 2000 所在系统分区，如图 C-4 所示。

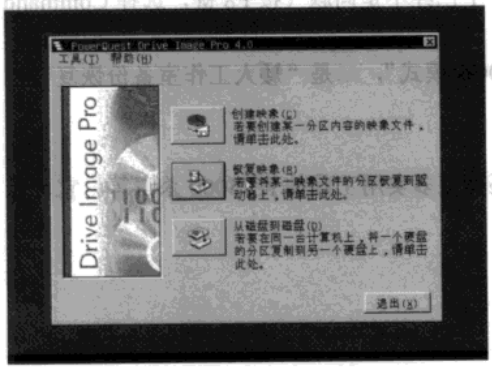


图 C-3

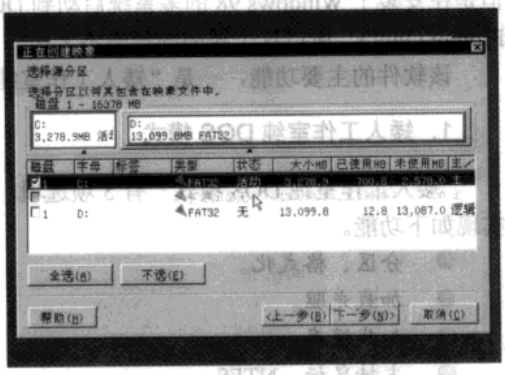


图 C-4

输入要创建的系统分区的映象文件名，并加以注释。这里输入“D:\2000.PQI”，即把映象文件创建到 D 盘根目录下，文件名为 2000.PQI，如图 C-5 所示。单击“下一步”按钮，提示选择压缩级别（高压缩比的创建速度慢，反之则快）。这里选择“低”选项，如图 C-6 所示。

单击“下一步”按钮显示创建映像文件的详细信息，如图 C-7 所示。确认无误后单击“完成”按钮开始创建，如图 C-8 所示。

根据系统分区大小，创建过程需要 10～20 分钟。映象文件创建完毕返回软件初始界面，等待用户执行其他操作。

如果单击软件初始界面中的“退出”按钮，将跳回 A 盘根目录下，如图 C-9 所示。在这里有很多强大的工具，比如长文件名支持工具、NTFS 分区支持工具、磁盘缓存工具、鼠标支持工具等。用户可根据需要选择使用。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

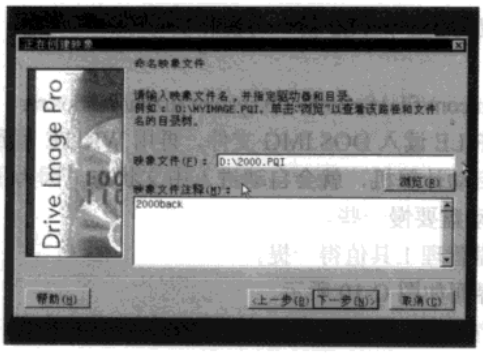


图 C-5

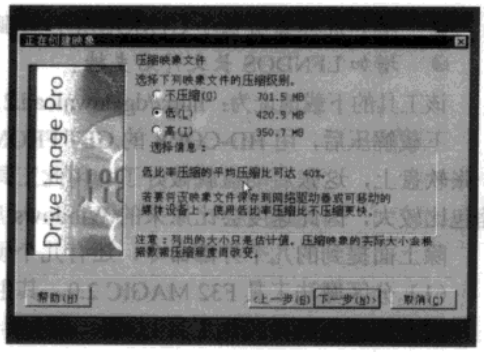


图 C-6

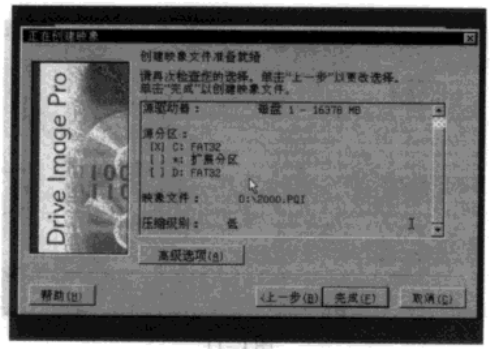


图 C-7

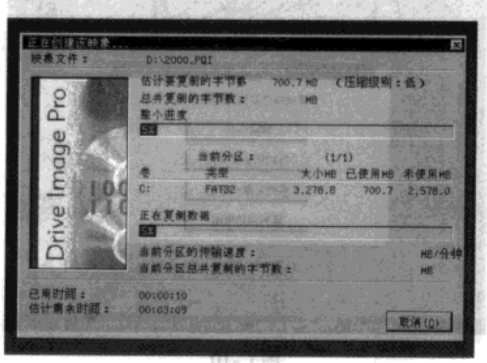


图 C-8

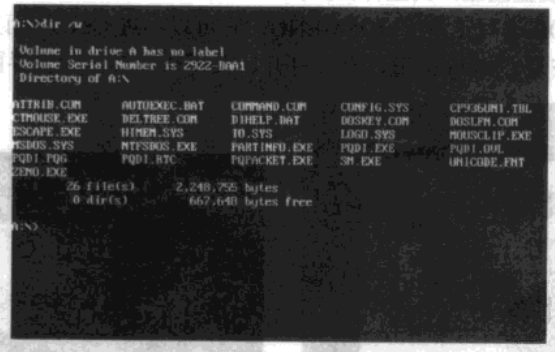


图 C-9

案例 121 梦幻中文 DOS 启动盘

梦幻中文 DOS 启动盘是在 Windows 98 启动盘的基础上制作的，保留了原启动盘的全部功能，支持大部分 IDE 光驱，并增加了一些新的特性。

- 用汉化的 Windows 98 FDISK 代替了原 FDISK，用户可以在自己熟悉的母语中进行分区操作。
- 从 FREEDOS 中补充了 XCOPY、DELTREE 两个常用的外部命令。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 增加鼠标驱动程序 CTMOUSE，可驱动 COM 和 PS2 接口的鼠标。
- 增加 LFNDOS 长文件名支持。

该工具的下载地址为：http://dg.download.21cn.com/file1farkoffsobb/system/fuzhu/ mhdos.rar。

下载解压后，用 HD-COPY 的 GET FROM FILE 读入 DOS.IMG 文件，再用 WRITE 写到一张软盘上，这张启动盘就做好了。用此工具启动计算机，就会自动进入中文状态。因为压缩包比较大，因此速度会比原来的 Windows 启动盘要慢一些。

除上面提到的几个外部命令，还有几个硬盘管理工具值得一提。

（1）分区魔法工具 F32 MAGIC 2.0，其主界面如图 C-10 所示。

（2）硬盘低级格式化工具 LOW，其主界面如图 C-11 所示。

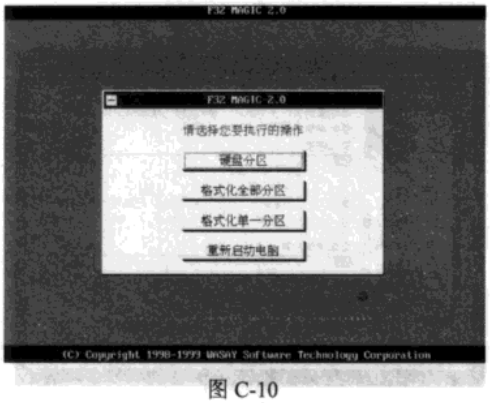


图 C-10

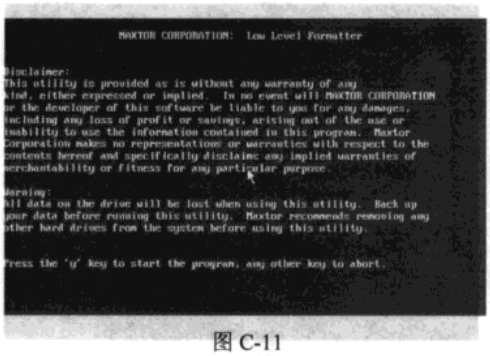


图 C-11

（3）著名的三茗硬盘医生，其主界面如图 C-12 所示。

（4）有一个 CMOS 读写工具 CMOSMENU，它可以不进 CMOS 而直接管理 CMOS（无需密码），如备份、恢复 CMOS 的值，直接打开、关闭软驱等，其主界面如图 C-13 所示。

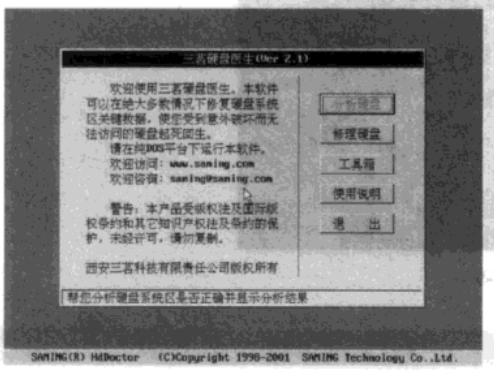


图 C-12

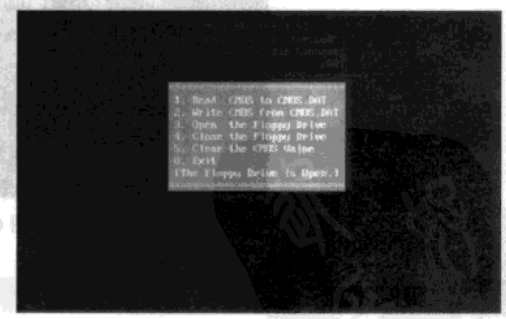


图 C-13

这些工具的使用都比较简单，读者可自己摸索。

案例 122　中文多功能 DOS 启动盘（识别闪存）3.0

中文多功能 DOS 启动盘也是一个综合了各种系统维护工具的启动盘，支持在 DOS 下使

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

用闪存盘。具体功能如下。

- 中文 FDISK 系统分区。
- Format 分区格式化。
- 中文 Diskman 查看并修复分区表，也可以备份分区表。
- KV3000 可以查杀引导区病毒。
- 可以识别闪存，并且可以用 FDISK 对闪存进行分区。

该的工具下载地址为：http://hld.onlinedown.net/down/K12RJ0000039581.exe。

下载完成后直接运行，当提示插入软盘时，插入一张格式化好的空白软盘，批处理程序会自动向软盘写入启动盘文件，如图 C-14 所示。

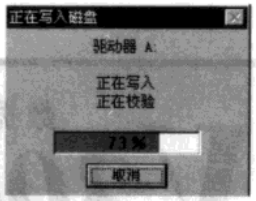


图 C-14

写完之后，一张多功能 DOS 启动盘就制作完成了。设置系统从软驱启动，进入到 A 盘下。

由于启动盘在 autoexec.bat 中加载了 tway 中文系统，所以用户可见到图 C-15 所示的中文显示界面。用“dir /w”查看，可看到很多附加工具，如图 C-16 所示。

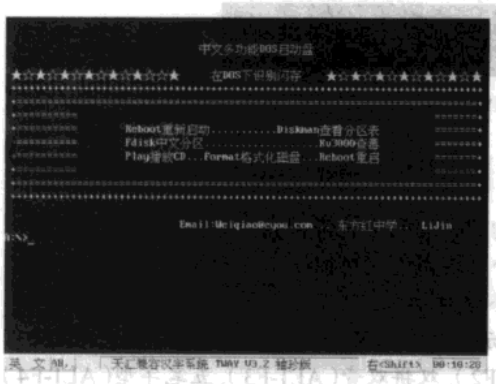


图 C-15

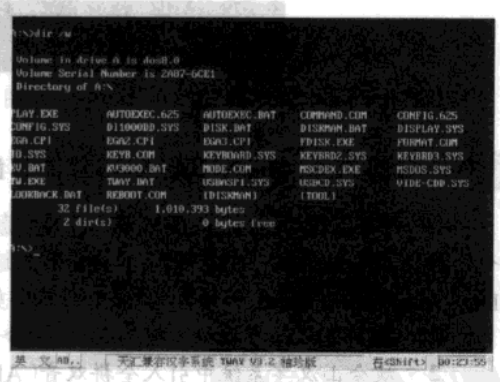


图 C-16

其中有一个“PLAY.EXE”。用此工具可以在 DOS 下欣赏音乐，这绝对是一件很“酷”的事情，如图 C-17 所示。

使用中文版的 FDISK 分区工具，看着中文提示进行分区操作就不易出错了，如图 C-18 所示。

运行 KV.BAT 或 KV3000.BAT 可通过批处理启动 KV3000 杀毒，如图 C-19 所示。

工具列表中，有两个带 USB 字样的 SYS 文件，它们是为了支持 USB 设备而使用的。

若需要在 DOS 下重启系统，直接键入 reboot 命令即可，因为它也是启动盘的工具之一。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

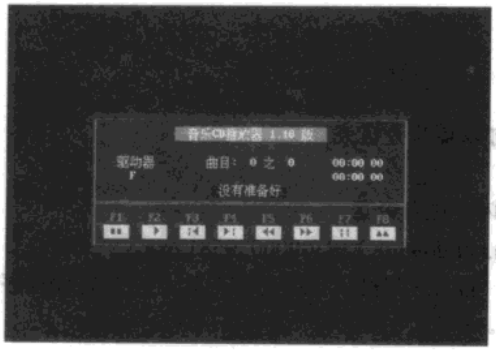


图 C-17

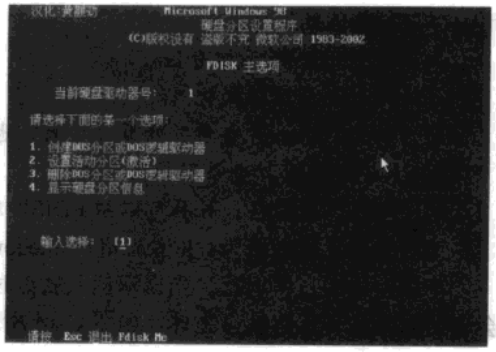


图 C-18



图 C-19

案例 123 中文多功能 DOS 启动 U 盘

“中文多功能 DOS 启动盘 U 盘”也是一款功能全面的系统维护盘，安装前把 U 盘分出一个至少 5.5M 的分区，然后把该工具安装到这个分区里面（可以用上文介绍的“中文多功能 DOS 启动盘”在 DOS 下分区）。该工具具备如下多种功能。

- 采用天汇汉字系统，可对 DOS 命令提示信息自动汉化。
- 从金山汉字系统中引入全拼双音（ALT-F2）、双拼双音（ALT-F3）、五笔字型（ALT-F4）几种输入法，加上自带的国标区位（ALT-F1），可满足大多数人的需要。
- Edit 中文编辑器。
- LOW 中文低格。
- HD-Copy 中文拷贝。
- Spfdisk 分区管理。
- Diskman 查看和备份分区表。
- KV2003DOS 查毒。
- Fdisk 中文分区。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- Backup 备份工具。
- Reboot，在 DOS 下重新启动。
- HDD 三茗中文硬盘检测修复工具，修复大部分硬盘软故障。
- F32 简体中文飞速分区、格式化工具。
- Cmos 非常好用的 CMOS 工具，可以备份/恢复 CMOS 信息及查 CMOS 密码。
- 超小型的 CD 播放器 PLAY。

下载地址：http://crc.onlinedown.net:82/down/DOS_U.exe。

首先运行 autoexec.bat 批处理文件，加载中文环境，显示主要工具菜单，如图 C-20 所示。中文界面的文本编辑器使用起来很方便，如图 C-21 所示。

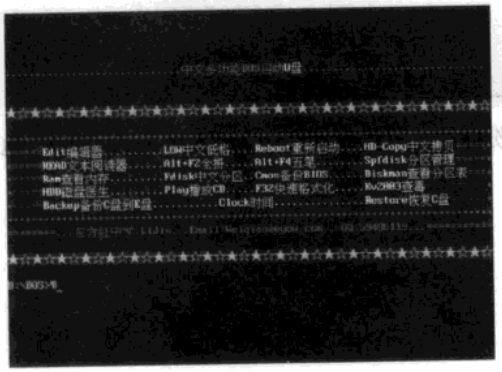


图 C-20

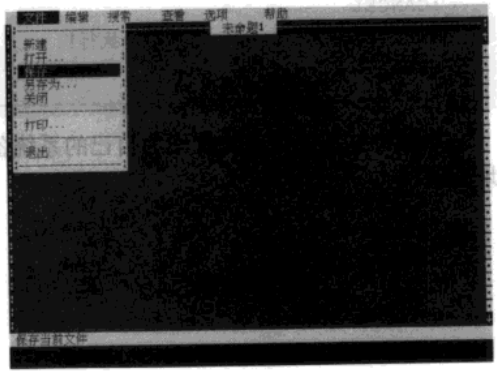


图 C-21

最实用的功能是自动备份的功能，只要运行 back.bat 批处理文件，即可自动对 C 盘备份，如图 C-22 所示。



图 C-22

要改变默认设置，用户可适当修改批处理文件，批处理源文件内容如下。

```
---------------------------------------------------------------
@SMARTDRV
@PDOS /NP
@CLS
@CLS
@WRITEXT 1 1 -f7 执行操作：制作镜像文件
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
@WRITEXT 2 1 -f7 操作目的：第 1 块硬盘的第 1 个分区的数据镜像为 -f9 E:\c-back.GHO
@WRITEXT 3 1 -f7 附加设置：快速压缩；自动确认；完成后重新启动
@WRITEXT 4 1 -f7 特别提示：-f12 E 盘必需要有足够的空间存放镜像文件!
@WRITEXT 5 1 -f15 按[Y]键开始，按[N]键取消。
@CHOICE
@If errorlevel 1 if not errorlevel 2 goto BEGIN
@if errorlevel 2 if not errorlevel 3 goto CANCEL
:BEGIN
@WRITEXT 0+ 1 -f14 已经开始执行，请稍等...
@GHOST -clone,mode=pdump,src=1:1,dst=E:\c-back.GHO -z2 -sure -rb
@goto END
:CANCEL
@WRITEXT 0+ 1 -f8 已经取消执行!
:END
-----------------------------------------------------------------
```

比如将默认的保存位置设为自己的系统备份路径，只需改动文中的“E:\c-back.GHO”地址即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



附录D 命令集

一、DOS 内、外部命令

DOS 内部命令

命　令	dir
功　能	显示指定目录下的所有文件、子目录和目录信息
命令格式	dir [盘符:][路径][文件名][参数]
参数解析	/w：宽屏显示，一排显示 5 个文件名，不显示修改时间和文件大小
	/p：分页显示，当屏幕无法将信息完全显示时，就分页显示
	/s：显示当前目录及其子目录下所有的文件，通过这个参数，可以进行某个文件或目录的查找，比如我们可以在 C:\>后输入“dir*. /来查找 C 盘中所有后缀名为 dat 的文件
	/a[:]属性：显示具有指定属性的文件。 h：显示隐藏文件。 s：显示系统文件。 d：显示目录。 -d：仅显示文件。 r：显示只读文件或文件夹。 -r：显示非只读文件或文件夹。 上述属性开关可以组合使用，但属性之间不能用空格分开
	/o[:]排序方式：按指定的“排序方式”显示文件和目录。 n：按文件名字母顺序排序。 d：按日期和时间的先后顺序排序。 s：按文件的大小排序，文件小的在前。 g：按目录在前、文件在后的顺序排序
命　令	md
功　能	建立目录
命令格式	md [盘符:][路径] [文件名]
说　明	不能在同一个磁盘的同一目录中，创建同名的子目录和同名的文件
命　令	rd
功　能	删除目录
命令格式	rd[盘符:][路径] [文件名]
说　明	该命令只能删除空目录，且不能删除当前目录

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

DOS 内部命令

命　令	cd
功　能	① 进入指定目录； ② 返回上级目录； ③ 返回到根目录
命令格式	cd [路径] [目录] cd.. cd\
命　令	**copy**
功　能	① 将文件拷贝到指定的目录下； ② 对指定的文件依次连接起来，拷贝到指定的文件中； ③ 通过键盘和屏幕建立 ASCII 码型的磁盘文件
命令格式	copy　<源文件名> [<目标文件名>] copy　<源文件名 1>+<源文件名 2>[+…] [<目标文件名>] copy　con：［<文件名全称>］
命　令	**del**
功　能	删除指定的文件
命令格式	del[盘符:][路径]〈文件名〉[/p]
参数解析	/p：系统在删除前询问是否真要删除该文件，若不使用这个参数，则自动删除
说　明	① 该命令不能删除属性为隐藏或只读的文件； ② 在文件名称中可以使用通配符
命　令	**ren**
功　能	更改文件名称
命令格式	ren[盘符:][路径]〈旧文件名〉〈新文件名〉
说　明	① 新文件名前不可以加上盘符和路径，因为该命令只能对同一盘上的文件更换文件名； ② 允许使用通配符（*、?），一次性更改一组相同的文件名或扩展名
命　令	**type**
功　能	显示 ASCII 码文件的内容
命令格式	type[盘符:][路径]〈文件名〉 type[盘符:][路径]〈文件名〉>prn
说　明	① 只能显示由 ASCII 码组成的文本文件，对.exe、.com 等为扩展名的文件，其内容是无法显示； ② 该命令一次只可以显示一个文件的内容，不能使用通配符； ③ 如果文件有扩展名，则必须将扩展名写上； ④ 当文件较长，一屏显示不下时，可以按以下格式显示：type[盘符:][路径]〈文件名〉\|more。more 为分屏显示命令，使用此参数后当满屏时会暂停，按任意键会继续显示
命　令	**prompt**
功　能	改变提示符形式
命令格式	prompt[参数]

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

DOS 内部命令	
命　令	prompt
参数解析	prompt pg：以当前目录名和>号为提示符，这是最常用的提示符
	prompt $t：表示时间
	prompt $d：表示日期
	prompt $$：表示$
	prompt $q：表示=
	prompt $v：表示当前版本
	prompt $l：表示<
	prompt $b：表示\|
	prompt $h：表示退位符
	prompt $e：表示 Esc 代表的字符 prompt $_ 表示回车换行
命　令	path
功　能	设定、显示和返回自动搜寻路径
命令格式	path〔<盘符>〕<路径> path〔<盘符>〕<路径>；〔<盘符>〕<路径>…… path；（返回到最初的无定义状态） path（显示当前的定义）
命　令	help
功　能	查看或显示 DOS 命令的详细资料
命令格式	help 或 help [DOS 命令]
命　令	vol
功　能	显示磁盘卷标号
命令格式	vol[盘符:]
说　明	省略盘符，显示当前驱动器卷标
命　令	cls
功　能	清除屏幕上所有的显示信息，光标置于屏幕左上角
命令格式	cls
命　令	ver
功　能	显示当前系统的版本号
命令格式	ver
命　令	date
功　能	设置或显示系统日期
命令格式	date [yy-mm-dd]
命　令	time
功　能	设置或显示系统时间
命令格式	time [hh:mm:ss.xx]
命　令	“<”重定向符
功　能	将指定文件的内容输入到特定文件中
命令格式	<　[<盘符>][<路径>]<文件名>[.<扩展名>]

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

DOS 内部命令

命　令	“>”重定向符	
功　能	① 把输出数据送到指定名称的新文件中。 ② 把输出数据累加到原有文件之后。 ③ 将输出数据送到指定外部设备	
命令格式	> [<盘符>][<路径>]<文件名>[.<扩展名>] >> [<盘符>][<路径>]<文件名>[.<扩展名>] > <设备名>	
命　令	“	”管道符
功　能	将前后两个命令连接起来	
命令格式	[<盘符>]	<DOS 命令>

DOS 外部命令

命　令	format
功　能	对磁盘进行高级格式化
命令格式	format〈盘符：〉
参数解析	/s：在对磁盘进行高级格式化时，将系统文件 io.sys 、msdos.sys 及 command.com 复制到磁盘上，使该磁盘可以作为 DOS 启动盘
	/v：在高级格式化全部完成前，系统要求给所格式化的磁盘起一个名字，称此名字为“磁盘卷标”
	/f:size：指定被格式化的软盘容量
	/q：快速格式化
	/u：无条件格式化，即破坏原来磁盘上所有数据
	/c：重新测试磁盘坏簇
命　令	unformat
功　能	恢复被高级格式化的磁盘中的数据
命令格式	unformat〈盘符〉
参数解析	/l：将列出找到的子目录名称、文件名称、文件日期等信息
	/p：将显示于屏幕的报告（包含/L 参数所产生的信息）同时也送到打印机。运行时屏幕会显示：“Print out will be sent to LPT1”
	/test：只做模拟试验（test），不做真正的写入动作。使用此参数屏幕会显示：“Simulation only”
	/u：不使用 mirror 映像文件的数据，直接根据磁盘现状进行 unformat
	/psrtn：修复硬盘分区表
说　明	① 盘符之后加上/p、/l、/test 之一，都相当于使用了/u 参数。 ② unformat 对于刚 format 的磁盘可以完全恢复，但 format 后若做了其他数据的写入，则 unformat 就不能完整地救回数据了。unformat 并非是万能的，由于使用 unformat 会重建 fat 与根目录，所以具有较高的危险性，操作不当可能会扩大损失。如果仅误删了几个文件或子目录，只需要利用 undelete 就够了
命　令	fdisk
功　能	对磁盘进行分区

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

DOS 外部命令

命　令	fdisk
命令格式	fdsik
命　令	xcopy
功　能	复制指定的目录和目录下的所有文件与目录结构
命令格式	xcopy [源盘:]〈源路径名〉[目标盘符:][目标路径名]
参数解析	/s：对目录下所有的子目录和文件进行拷贝
	/v：对拷贝的目标盘进行检查，以提高拷贝的可靠性
	/p：在拷贝的过程中对每个源文件进行询问，以确认是否真正拷贝
	/w：提供一行等待信息，以便用户更换磁盘
	/d:日期：只拷贝指定<日期>及此<日期>之后建立或修改过的文件
命　令	diskcopy
功　能	对指定磁盘进行全盘复制
命令格式	diskcopy [盘符 1:][盘符 2:]
参数解析	/1：只拷贝磁盘的单面
	/v：校验 copy 的信息是否正确。使用此参数将降低 copy 的速度
命　令	deltree
功　能	删除整个目录命令
命令格式	deltree[盘符：]〈路径名〉
说　明	该命令可以就将目录及其下的所有文件（包括隐藏、系统、只读文件）、子目录、一次性删除。操作时，一定要慎重
命　令	undelete
功　能	恢复被误删除命令
命令格式	undelete[盘符:][路径名]〈文件名〉
参数解析	/dos：根据目录里残留的记录来恢复文件
	/list：只“列出”符合指定条件的文件而不做恢复，所以对磁盘内容完全不会有影响
	/all：自动将可完全恢复的文件完全恢复，而不一一地询问用户
命　令	attrib
功　能	修改指定文件的属性
命令格式	attrib[文件名][r][-r][a][-a][h][-h][s][-s][/s]
参数解析	/r：将指定文件设为只读属性
	-r：去除只读属性
	a：将文件设置为档案属性
	-a 参数：去除档案属性
	h：将文件调协为隐含属性
	-h：去隐含属性
	s：将文件设置为系统属性
	-s：去除系统属性
	/s 参数，对当前目录下的所有子目录及作设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

DOS 外部命令

命　令	mem
功　能	显示当前内存使用的情况
命令格式	mem[参数]
参数解析	/c：列出装入常规内存和 cmb 的各文件的长度，同时也显示内存空间的使用状况和最大的可用空间
	/f：分别列出当前常规内存剩余的字节大小和 umb 可用的区域及大小
	/m：显示该模块使用内存地地址、大小及模块性质
	/p：指定当输出超过一屏时，暂停以供用户查看
命　令	chkdsk
功　能	显示磁盘状态、内存状态和指定路径下指定文件的不连续数目
命令格式	chkdsk[盘符:][路径][文件名]
参数解析	/f：纠正在指定磁盘上发现的逻辑错误
	/v：显示盘上的所有文件和路径
命　令	scandisk
功　能	检测磁盘的 fat 表、目录结构、文件系统等是否有问题，并可将检测出的问题加以修复
命令格式	scandisk[盘符 1:]{[盘符 2:]…}
参数解析	/fragment［驱动器名:\路径\文件名］：使用这个参数可以显示文件是否包含有间断的块，可以通过运行磁盘整理程序来解决这个问题
	/all：检查并修复所有的本地驱动器错误
	/autofix：自动修复错误，修复时不会出现提示
	/checkonly：仅仅检查磁盘，并不修复错误
	/custom：根据 Scandisk.ini 文件的内容来运行 Scandisk。Scandisk.ini 是一个文本文件，它包含了对 Scandisk 程序的设置，其中的［custom］块是在加上“/custom”参数后才执行的，用户可以根据自己的不同情况来进行不同的设置
	/nosave：在检查出有丢失簇后直接删除，并不转化为文件
	/nosummary：不显示检查概要，完成检查后直接退出程序
	/surface：在完成初步检查后进行磁盘表面扫描
	/mono：以单色形式运行 Scandisk
说　明	① scandisk 适用于硬盘和软盘，可以一次指定多个磁盘或选用[/all]参数指定所有的磁盘。 ② 可自动检测出磁盘中所发生的交叉连接、丢失簇和目录结构等逻辑上的错误，并加以修复
命　令	smartdrv
功　能	磁盘性能加速
命令格式	smartdrv[参数]
参数解析	/x：执行并驻留内存，开辟磁盘加速缓存区，并屏蔽所有驱动器缓存
	/c：将缓存内的信息都写入硬盘
	/e:数字：设置一次移动的信息量
	/b:数字：设置预先读取的缓冲区大小

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

DOS 外部命令

命　令	defrag
功　能	整理磁盘，消除磁盘碎片
命令格式	defrag[盘符:]
参数解析	/f：消除磁盘上的碎片，并对磁盘文件进行重新整理，确保文件之间毫无空隙。从而加快读盘速度和节省磁盘空间
命　令	sys
功　能	将当前驱动器上的 dos 系统文件 io.sys、msdos.sys 和 command.com 传送到指定的驱动器上
命令格式	sys[盘符:]
命　令	more
功　能	从标准输入设备读数据，并在屏幕上显示信息
命令格式	more
命　令	edit
功　能	编辑文本
命令格式	edit[文件名]
命　令	sort
功　能	对数据进行排序
命令格式	sort[参数]
参数解析	/r：进行逆排序
	/+n：以每一数据行的第 n 列开始作为排序的依据，如果不引用此开关则以第 1 列为依据
命　令	tree
功　能	显示磁盘目录结构
命令格式	tree[盘符:]
参数解析	/f：显示所有目录及目录下的所有文件。省略时，只显示目录，不显示目录下的文件
	>prn：把所列目录及目录中的文件名打印输出
命　令	label
功　能	建立、更改、删除磁盘卷标
命令格式	label[盘符：][卷标名]
命　令	find
功　能	从指定的 1 至若干个文件或标准输入设备中，按<字符串>和可选择的开关，查找出符合条件的文本行
命令格式	find [参数]<“字符串”>[<文件名全称>…]
参数解析	/v：则把文件中不含有指定字符串的文本行筛选出来，并在标准输出显示
	/c：只显示符合条件的文本行的行数
	/n：使所输出的文本行前都包括有各自在文本中的顺序号
命　令	fc
功　能	比较文件的异同，并列出差异处
命令格式	fc[盘符:][路径名]〈文件名〉[盘符:][路径名][文件名]

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

DOS 外部命令

命　令	fc
参数解析	/a：为 ASCII 码比较模式
	/b：为二进制比较模式
	/c：将大小写字符看成是相同的字符
	/n：在 ascii 码比较方式下，显示相异处的行号
命　令	**diskcomp**
功　能	比较两张磁盘内容是否相同
命令格式	diskcomp[盘符 1] [盘符 2]
命　令	**restore**
功　能	将备份盘上备份文件恢复到指定盘上
命令格式	restore[备份盘符] [目标盘符] [参数]
参数解析	/s：将备份文件包括子目录都恢复到指定盘上
	/p：让用户判断是否恢复文件
	/b:日期：恢复日期以前的文件
	/a:日期：恢复日期之后的文件
	/l:时间：恢复时间之前的文件
	/e:时间：恢复时间之后的文件
	/m：只恢复上次备份后修改过的文件
	/n：只恢复上次备份后已删除的文件
	/d：只显示要恢复的文件名
命　令	**append**
功　能	设置非执行文件的路径
命令格式	append[路径];[路径]
命　令	**msd**
功　能	显示系统的硬件和操作系统的状况
命令格式	msd[参数]
参数解析	/i：不检测硬件
	/b：以黑白方式启动 MSD
	/s：显示出简明的系统报告
命　令	**debug**
功　能	备份/恢复主引导分区、分区表，以及调试程序
命令格式	① debug ② debug [[驱动器号:][路径]文件名[调试参数]]
命　令	**fasthelp**
功　能	快速显示帮助信息
命令格式	① fasthelp ② fasthelp [DOS 命令]
命　令	**expand**
功　能	对文件进行解压缩

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

DOS 外部命令	
命　令	expand
命令格式	expand[源文件名] [目的文件]
命　令	vsafe
功　能	在 DOS 下对电脑进行病毒防护
命令格式	vsafe vsafe[参数]
参数解析	/u：从内存中去除 vsafe /ne：将 vsafe 装入扩充内存 /nx：将 vsafe 装入扩展内存

二、“批处理文件”命令

“批处理文件”命令	
命　令	echo
功　能	显示与不显示命令后的字符
命令格式	echo：表示显示此命令后的字符。 echo off：表示在此语句后所有运行的命令都不显示命令行本身
命　令	@
功　能	与 echo off 相似，但它是加在其他命令行的最前面，表示运行时不显示命令行本身
命令格式	@
命　令	call
功　能	调用另一条批处理文件
命令格式	call [盘符:][路径][文件名]
命　令	pause
功　能	运行此句会暂停，显示“Press any key to continue...”，等待用户按任意键后继续。
命令格式	pause
命　令	rem
功　能	此命令后的字符为解释行，不执行
命令格式	rem
命　令	if
功　能	判断条件命令
命令格式	① if "参数" == "字符串" [待执行的命令]：表示参数如果等于指定的字符串，则条件成立，运行命令；否则运行下一句（注意参数后面是两个等号）。 ② if exist 文件名 [待执行的命令]：如果有指定的文件，则条件成立，运行命令；否则运行下一句。 ③ if errorlevel 数字 [待执行的命令]：如果返回码等于指定的数字，则条件成立，运行命令；否则运行下一句
命　令	goto
功　能	跳转语句

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

“批处理文件”命令	
命　令	goto
命令格式	goto end :end
命　令	for
功　能	循环语句
命令格式	for [%%f] in （集合）do[命令]
命　令	choice
功　能	使用此命令可以让用户输入一个字符，从而运行不同的命令
命令格式	choice /c: [字符]
参数解析	/c：表示在此后应给出提示，并输入字符

三、“系统恢复控制台”命令

“系统恢复控制台”命令	
命　令	attrib
功　能	更改单个文件或目录的属性
命令格式	attrib [+r\|-r] [+s\|-s] [+h\|-h] [+c\|-c] [盘符:] [路径] [文件名]
参数解析	+r：设置只读属性
	-r：清除只读属性
	+s：设置系统属性
	-s：清除系统属性
	+h：设置隐藏属性
	-h：清除隐藏属性
	+c：设置压缩属性
	-c：清除压缩属性
说　明	可以用一个命令更改一个文件或目录的多个属性
命　令	batch
功　能	执行在文本文件中指定的命令
命令格式	batch input_file [output_file]
参数解析	input_file：指定包含要执行的命令列表的文本文件。input_file 可以由驱动器号和冒号、目录名、文件名或它们的组合构成
	output_file：如果指定，则在命名文件中存储命令输出。如果没有指定，输出将显示在屏幕上
说　明	批处理文件不能包含嵌套的 batch 命令
命　令	chdir（cd）
功　能	显示当前目录的名称，或更改当前的文件夹
命令格式	chdir[盘符:] [路径] [..]
参数解析	[..]：指明要改到父文件夹。在 chdir 和两点之间插入一个空格
说　明	① chdir 将空格视作分隔符。用引号将包含空格的目录名扩起来。例如：chdir "盘符 r cache"。 ② chdir 只适用于当前 Windows 安装的系统目录、可移动媒体、硬盘分区的根目录或本地安装源

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

“系统恢复控制台”命令

命　令	copy
功　能	① 将单个文件复制到其他位置。 ② 含有特殊参数的 copy 命令仅在使用故障恢复控制台时才可用。 ③ 可在命令提示符下使用带不同参数的 copy 命令
命令格式	copy source [destination]
参数解析	source：指定要被复制的文件的位置和名称。source 可由驱动器号和冒号、目录名、文件名或组合所组成
	destination：指定要复制到其中的文件或文件集的位置和名称。destination 可以由驱动器号和冒号、文件夹名、文件名及组合而组成
说　明	① 源可以是可移动媒体、当前 Windows 安装的系统目录中的任何目录、驱动器的根目录、本地安装源或 CMDCONS 目录。 ② 目标可以是除可移动媒体以外的任何与源相同的位置。如果没有指定目标，则默认为当前目录。 ③ copy 不支持通配符
命　令	delete（del）
功　能	删除单个文件
命令格式	del[盘符:] [路径] 文件名
命　令	dir
功　能	显示目录中的文件和子目录列表
命令格式	dir[盘符:] [路径] [文件名]
命　令	expand
功　能	从压缩文件中提取文件
命令格式	expand source [/F:filespec] [destination] [/d] [/y]
参数解析	source：指定要展开的文件。如果源文件只包含一个文件，请使用该选项。source 可由驱动器号和冒号、目录名、文件名或其组合所组成。不能使用通配符
	/f:size：如果源文件包含多个文件，指定要提取的文件的名称。可以对要提取的文件使用通配符
	destination：指定提取文件或每个单独文件的目标目录和（或）文件名
	/d：列出 CAB 文件中包含的文件而不展开或提取
	/y：在展开或提取文件时不出现覆盖提示
说　明	① 如果没有指定目标，文件将被复制到当前目录。 ② 不能将软盘驱动器或 CD-ROM 等可移动媒体指定为目标
命　令	mkdir（md）
功　能	创建目录或子目录。
命令格式	mkdir[盘符:] 路径
参数解析	盘符：指定要创建新目录的驱动器
	路径：指定新目录的名称和位置。不能使用通配符
命　令	rename（ren）
功　能	更改单个文件的名称
命令格式	rename[盘符:] [路径]文件名 1 文件名 2
命　令	rmdir（rd）
功　能	删除目录

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

“系统恢复控制台”命令

命　令	rmdir（rd）			
命令格式	rmdir　[盘符:] [路径]			
参数解析	[盘符:] [路径]：指定要删除的目录的位置和名称。不能使用通配符			
命　令	type			
功　能	显示文本文件的内容			
命令格式	type[盘符:] [路径] <文件名>			
命　令	more			
功　能	显示文本文件的内容			
命令格式	more[盘符:] [路径] <文件名>			
命　令	bootcfg			
功　能	启动配置和故障恢复（对于大多数计算机，即 boot.ini 文件）			
命令格式	bootcfg /default/add/rebuild			
参数解析	/default：设置默认引导项			
	/add：向引导列表中添加 Windows 安装			
	/rebuild：重复全部 Windows 安装过程并允许用户选择要添加的内容			
	/scan：扫描用于 Windows 安装的所有磁盘并显示结果			
	/list：列出引导列表中已有的条目			
	/disableredirect：在启动引导程序中禁用重定向			
	/redirect [PortBaudRrate]][useBiosSettings]：在启动引导程序中通过指定配置启用重定向			
说　明	① 使用/rebuild 参数之前，应先通过 bootcfg /copy 命令备份 boot.ini 文件 ② 使用/scan 参数扫描结果被静态存储，并用于本次会话。如果在本次会话期间磁盘配置发生变化，为获得更新的扫描结果，必须先重新启动计算机，然后再次扫描磁盘			
命　令	chkdsk			
功　能	创建并显示磁盘的状态报告			
命令格式	chkdsk[盘符:] [/p] [/r]			
参数解析	/p：即使驱动器不在 chkdsk 的检查范围内，也执行彻底检查。该参数不对驱动器做任何更改			
	/r：找到坏扇区并恢复可读取的信息。隐含着/p 参数			
说　明	chkdsk 命令需要 Autochk.exe 文件。如果不能在启动目录（默认为 \%systemroot%\System32）中找到该文件，将试着在 Windows 安装盘中找到它。如果有多引导系统的计算机，必须保证是在包含 Windows 的驱动器上使用该命令			
命　令	diskpart			
功　能	创建或删除硬盘驱动器上的分区			
命令格式	diskpart [/add	/delete] [device_name	drive_name	partition_name] [size]
参数解析	/add：创建新的分区			
	/delete：删除现有分区			
	device_name：要创建或删除分区的设备。设备名称可从 map 命令的输出获得。例如，设备名称为“\Device\HardDisk0”			
	drive_name：以驱动器号表示的待删除分区。仅与 /delete 同时使用			

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

“系统恢复控制台”命令

命　令	diskpart
参数解析	partition_name：以分区名称表示的待删除分区。可代替 drive_name 使用。仅与 /delete 同时使用。以下是分区名称的范例： \Device\HardDisk0\Partition1
	size：要创建的分区大小，以兆字节（MB）表示。仅与 /add 同时使用
命　令	fixboot
功　能	向系统分区写入新的分区引导扇区
命令格式	fixboot[盘符:]
说　明	如果不带任何参数，fixboot 命令将向用户登录的系统分区写入新的分区引导扇区
命　令	fixmbr
功　能	修复启动磁盘的主启动记录
命令格式	fixmbr[device_name]
参数解析	device_name：要写入新的主引导记录的设备（驱动器）。设备名称可从 map 命令的输出获得。例如，设备名称为“\Device\HardDisk0”
说　明	① 如果不指定 device_name，新的主引导记录将被写入引导设备，即装载主系统的驱动器。 ② 如果系统检测到无效或非标准分区表标记，将提示用户是否继续执行该命令。除非您访问驱动器有问题，否则不要继续进行。向系统分区写入新的主引导记录可能破坏分区表并导致分区无法访问
命　令	format
功　能	将指定的驱动器格式化为指定的文件系统
命令格式	format [盘符:] [/fs:file-system]
参数解析	/q：对驱动器进行快速格式化。不扫描驱动器，因此只应对格式化过的驱动器使用此参数
	/fs:file-system：指定要使用的文件系统，如 FAT、FAT32 或 NTFS。如果未指定文件系统，将使用现有的文件系统格式
命　令	map
功　能	显示驱动器号与物理设备名称的映射。该信息在运行 fixboot 和 fixmbr 命令时非常有用
命令格式	map[arc]
参数解析	arc：指示 map 命令显示高级 RISC 计算（ARC）设备名称
说　明	如果不使用 arc 参数，则 map 命令显示设备名称
命　令	cls
功　能	清除屏幕
命令格式	cls
命　令	disable
功　能	禁用 Windows XP、Windows 2000 或 Windows NT 4.0 系统服务或设备驱动程序
命令格式	disable{service_name]][device_driver_name}
参数解析	service_name：要禁用的系统服务名称
	device_driver_name：要禁用的设备驱动程序名称
命　令	enable
功　能	启用 Windows XP、Windows 2000 或 Windows NT 4.0 系统服务或设备驱动程序

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

“系统恢复控制台”命令	
命　令	enable
命令格式	enable {service_name \|device_driver_name}[startup_type]
参数解析	service_name：要启用的系统服务的名称
	device_driver_name：要启用的设备驱动程序的名称
	startup_type：要为服务或设备驱动程序指派的启动类型。有效的启动类型包括： service_boot_start service_system_start service_auto_start service_demand_start
说　明	① 如果不指派启动类型，enable 命令将列出在 service_name 中指定的服务或设备驱动程序的当前启动类型。 ② 使用 enable 命令更改启动类型时，上次启动类型的名称将显示在屏幕上。应该记下该名称，以便在需要时将启动类型恢复为上次的设置
命　令	exit
功　能	关闭故障恢复控制台并重新启动计算机
命令格式	exit
命　令	help
功　能	提供有关故障恢复控制台命令的联机信息
命令格式	help [commandname]
参数解析	commandname：提供有关命令信息，包括命令使用的参数
命　令	listsvc
功　能	列出计算机上可以使用的服务和驱动程序
命令格式	listsvc
命　令	logon
功　能	登录到 Windows 安装
命令格式	logon
说　明	① logon 命令将列出所有检测到安装的 Windows 系统，输入本地管理员密码才能登录。 ② 如果 3 次登录尝试都失败，“故障恢复控制台”会自动关闭，且重新启动计算机
命　令	net use
功　能	将网络共享连接到驱动器号
命令格式	net use [\\ComputerName\ShareName[/user:[DomainName\]UserName]password] \|[driveletter:] [/d]
参数解析	\\ServerName\ShareName：指定服务器和共享资源的名称
	/user：指定建立连接的用户名
	DomainName：确认用户的凭据时所要使用的域名
	UserName：指定登录时使用的用户名
	password：指定访问共享资源所需的密码。不输入密码，将给出要键入密码的提示。在密码提示行处键入密码时不显示密码
	/d：表示将不断开该连接

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

“系统恢复控制台”命令	
命　令	set
功　能	显示和设置“故障恢复控制台”的环境变量。set 命令是必须与安全模板一同使用的可选命令
命令格式	set[variable=[string]]
参数解析	variable：指定需要设置或修改的变量
	“故障恢复控制台”支持以下环境变量。 ① AllowWildCards：允许某些命令支持通配符。 ② AllowAllPaths：允许访问系统上的所有文件和目录。 ③ AllowRemovableMedia：允许文件复制到可移动媒体上，如软盘。 ④ NoCopyPrompt：覆盖现有文件时不显示提示
	string：指定要与指定变量关联的字符串
说　明	目录必须为空，否则命令失败
命　令	systemroot
功　能	将当前目录设置为用户登录到的 Windows 安装系统的 systemroot 文件夹
命令格式	systemroot

四、“命令提示符”命令

“命令提示符”命令	
命　令	dir
功　能	显示指定目录下的所有文件、子目录和目录信息
命令格式	dir[盘符:][路径][文件名][参数]
增强参数	/-c：取消显示中的分隔符，以满足部分人的视觉习惯
	/q：显示文件、目录的用户属性
	/t:c：显示文件、显示目录的创建时间
	/t:a：显示上次访问时间
	/t:w：显示上次修改时间
	/x：使用此参数即“dir/x”列文件、目录时，会对长文件名同时显示“8.3”格式的文件名
命　令	del（erase）
功　能	删除文件
命令格式	del [/p] [/f] [/s] [/q] [/a[[:]attributes]] [names]
增强参数	/p：删除每一个文件之前提示确认
	/s：从子目录中删除指定文件
	/q：安全模式
	/a：根据属性选择要删除的文件
命　令	cd（chdir）
功　能	进入指定的目录
命令格式	chdir [/d] [drive:][path]
增强参数	/d：快速改变当前目录

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

“命令提示符”命令

命　令	color				
功　能	改变命令提示符的前景和背景颜色				
命令格式	color[attr]				
增强参数	attr：指定控制台输出的颜色属性。颜色属性由两个十六进制数字指定：第一个为背景，第二个则为前景。每个数字可以为以下任何值之一： 0＝ 黑色　8＝ 灰色 1＝ 蓝色　9＝ 淡蓝色 2＝ 绿色　A＝ 淡绿色 3＝ 湖蓝色　B＝ 淡浅绿色 4＝ 红色　C＝ 淡红色				
命　令	color				
增强参数	5＝ 紫色　D＝ 淡紫色 6＝ 黄色　E＝ 淡黄色 7＝ 白色　F＝ 亮白色				
命　令	md（mkdir）				
功　能	建立目录				
命令格式	md[盘符:]<路径>				
说　明	在命令提示符下，此命令一次性可以建立多级目录				
命　令	rd				
功　能	删除目录				
命令格式	rd[盘符:]<路径>				
增强参数	/s：可以删除目录树，即删除目录及目录下的所有子目录和文件，相当于以前版本中的 deltree 命令				
增强参数	/q：使用上面的/S 参数删除目录树时，系统会要求用户确认是否真的要删除。若同时使用/Q 参数，即“rd/s /q”，在进行删除操作时将取消确认，相当于 deltree 命令的/Y 参数				
命　令	attrib				
功　能	更改文件或目录的属性				
命令格式	attrib [+r	-r] [+s	-s] [+h	-h] [+c	-c] [盘符:] [路径] [文件名]
增强参数	/d：在 Windows XP 中我们不能把文件或文件夹设置为系统属性，只能设为只读、隐藏或存档属性。而带参数/d 使用 attrib 命令可以对文件的所有属性进行设定，设定时必须与参数/s 同时使用				
命　令	format				
功　能	对磁盘进行高级格式化				
命令格式	format[盘符:]				
增强参数	/fs:filessystem：按指定文件系统类型（FAT、FAT32、NTFS）格式化磁盘，例如“format /fs:NTFS”				
命　令	convert				
功　能	将 FAT32 文件系统转换为 NTFS 文件系统				
命令格式	convert[盘符] /fs:ntfs				

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

“命令提示符”命令

命　令	ping
功　能	用于检测网络连接性、可到达性和名称解析的疑难问题的主要 TCP/IP 命令
命令格式	ping[-t] [-a] [-n Count] [-l Size] [-f] [-i TTL] [-v TOS] [-r Count] [-s Count] [{-j HostList \| -k HostList}] [-w Timeout] [TargetName]
参数解析	-t：指定在中断前 ping 可以持续发送回响请求信息到目的地。要中断并显示统计信息，请按“CTRL+BREAK”组合键。要中断并退出 ping，请按“CTRL+C”组合键
	-a：指定对目的地 IP 地址进行反向名称解析。如果解析成功，ping 将显示相应的主机名
	-n Count：指定发送回响请求消息的次数，默认值为 4
	-l Size：指定发送的回响请求消息中“数据”字段的长度（以字节表示），默认值为 32，Size 的最大值是 65,527
	-f：指定发送的回响请求消息带有“不要拆分”标志（所在的 IP 标题设为 1）。回响请求消息不能由目的地路径上的路由器进行拆分。该参数可用于检测并解决“路径最大传输单位（PMTU）”的故障
	-i TTL：指定发送回响请求消息的 IP 标题中的 TTL 字段值。其默认值是是主机的默认 TTL 值。对于 Windows XP 主机，该值一般是 128。TTL 的最大值是 255
	-v TOS：指定发送回响请求消息的 IP 标题中的“服务类型（TOS）”字段值。默认值是 0。TOS 被指定为 0 到 255 的十进制数
	-r Count：指定 IP 标题中的“记录路由”选项用于记录由回响请求消息和相应的回响应答消息使用的路径。路径中的每个跃点都使用“记录路由”选项中的一个值。如果可能，可以指定一个等于或大于来源和目的地之间跃点数的 Count。Count 的最小值为 1，最大值为 9
	-s Count：指定 IP 标题中的“Internet 时间戳”选项用于记录每个跃点的回响请求消息和相应的回响应答消息的到达时间。Count 的最小值必须为 1，最大值为 4
	-j HostList：指定回响请求消息使用带有 HostList 指定的中间目的地集的 IP 标题中的“稀疏资源路由”选项。可以由一个或多个具有松散源路由的路由器分隔连续中间的目的地。主机列表中的地址或名称的最大数为 9，主机列表是一系列由空格分开的 IP 地址（带点的十进制符号）
	-k HostList：指定回响请求消息使用带有 HostList 指定的中间目的地集的 IP 标题中的“严格来源路由”选项。使用严格来源路由，下一个中间目的地必须是直接可达的（必须是路由器接口上的邻居）。主机列表中的地址或名称的最大数为 9，主机列表是一系列由空格分开的 IP 地址（带点的十进制符号）
	-w Timeout：指定等待回响应答消息响应的时间（以微秒计），该回响应答消息响应接收到的指定回响请求消息。如果在超时时间内未接收到回响应答消息，将会显示“请求超时”的错误消息。默认的超时时间为 4000（4 秒）
	TargetName：指定目的端，它既可以是 IP 地址，也可以是主机名
	/?：在命令提示符显示帮助
命　令	set
功　能	显示、设置或删除环境变量。如果没有任何参数，set 命令将显示当前环境设置
命令格式	set[[/a [expression]] [/p [variable=]] string]

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

“命令提示符”命令

命　令	set
增强参数	/a：将 string 设置成可求值的数字表达式
	/p：将 variable 的值设置成输入行
	variable：指定需要设置或修改的变量
	string：指定要与指定变量关联的字符串
命　令	**arp**
功　能	显示和修改“地址解析协议（ARP）”缓存中的项目
命令格式	arp [-a [InetAddr] [-N IfaceAddr]] [-g [InetAddr] [-N IfaceAddr]] [-d InetAddr [IfaceAddr]] [-s InetAddr EtherAddr [IfaceAddr]]
参数解析	-a [InetAddr] [-N IfaceAddr]：显示所有接口的当前 ARP 缓存表。要显示指定 IP 地址的 ARP 缓存项，请使用带有 InetAddr 参数的 arp -a，此处的 InetAddr 代表指定的 IP 地址；要显示指定接口的 ARP 缓存表，请使用-N IfaceAddr 参数，此处的 IfaceAddr 代表分配给指定接口的 IP 地址。-N 参数区分大小写
	-g [InetAddr] [-N IfaceAddr]：与-a 相同
	-d InetAddr [IfaceAddr]：删除指定的 IP 地址项，此处的 InetAddr 代表 IP 地址。对于指定的接口，要删除表中的某项，请使用 IfaceAddr 参数，此处的 IfaceAddr 代表分配给该接口的 IP 地址。要删除所有项，请使用星号通配符（*）代替 InetAddr
	-s InetAddr EtherAddr [IfaceAddr]：向 ARP 缓存添加可将 IP 地址 InetAddr 解析成物理地址 EtherAddr 的静态项。要向指定接口的表添加静态 ARP 缓存项，请使用 IfaceAddr 参数，此处的 IfaceAddr 代表分配给该接口的 IP 地址
命　令	**cprofile**
功　能	清除浪费空间的指定配置文件，如果用户特定文件关联是禁用的，则从注册表中删除这些文件关联。目前正在使用的配置文件没有修改
命令格式	cprofile [/l] [/i] [/v] [FileList]
参数解析	/l：清除所有本地配置文件。也可以在 FileList 参数中指定其他配置文件的列表
	/i：每个配置文件都交互式地提示用户
	/v：显示关于要执行的操作的信息
	FileList：要从中删除用户特定文件关联的文件的列表。用空格隔开列表中的每个文件。文件名中可以包含通配符字符
命　令	**ftp**
功　能	是将文件传输到运行文件传输协议（FTP）服务器服务（如 Internet 信息服务）的计算机，或从这台计算机传输文件。可以通过处理 ASCII 文本文件交互式地或以批处理模式使用 FTP
命令格式	ftp [-v] [-d] [-i] [-n] [-g] [-s:FileName] [-a] [-w:WindowSize] [-A] [Host]
参数解析	-v：禁止显示 FTP 服务器响应
	/d：启用调试、显示在 FTP 客户端和 FTP 服务器之间传递的所有命令
	-i：传送多个文件时禁用交互提示
	-n：在建立初始连接后禁止自动登录功能
	-g：禁用文件名组合

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

“命令提示符”命令	
命　令	ftp
参数解析	-s:FileName：指定包含 FTP 命令的文本文件。这些命令在启动 FTP 后自动运行。该参数不允许带有空格。使用该参数而不是重定向（<）
	-a：指定绑定 FTP 数据连接时可以使用任何本地接口
	-w:WindowSize：指定传输缓冲的大小。默认窗口大小为 4096 字节
	-A：匿名登录到 FTP 服务器
	Host：指定要连接的计算机名、IP 地址或 FTP 服务器的 IPv6 地址。如果指定了主机名或地址，则其必须是命令行的最后一个参数
命　令	ipconfig
功　能	显示所有当前的 TCP/IP 网络配置值、刷新动态主机配置协议（DHCP）和域名系统（DNS）设置。使用不带参数的 IPCONFIG 可以显示所有适配器的 IP 地址、子网掩码、默认网关
命令格式	ipconfig[/all] [/renew [adapter]] [/release [adapter]] [/flushdns] [/displaydns] [/registerdns] [/showclassid adapter] [/setclassid adapter [ClassID]]
参数解析	/all：显示所有适配器的完整 TCP/IP 配置信息。在没有该参数的情况下 ipconfig 只显示 IP 地址、子网掩码和各个适配器的默认网关值。适配器可以代表物理接口（例如安装的网络适配器）或逻辑接口（例如拨号连接）
	/renew [adapter]：更新所有适配器（如果未指定适配器），或特定适配器（如果包含了 adapter 参数）的 DHCP 配置。该参数仅在具有配置为自动获取 IP 地址的网卡的计算机上可用。要指定适配器名称，请键入不带参数的 ipconfig 命令显示的适配器名称
	/release [adapter]：发送 DHCPRelease 消息到 DHCP 服务器，以释放所有适配器（如果未指定适配器）或特定适配器（如果包含了 adapter 参数）的当前 DHCP 配置并丢弃 IP 地址配置。该参数可以禁用配置为自动获取 IP 地址的适配器的 TCP/IP。要指定适配器名称，请键入不带参数的 ipconfig 命令显示的适配器名称
	/flushdns：清理并重设 DNS 客户解析器缓存的内容。如有必要，在 DNS 疑难解答期间，可以使用本过程从缓存中丢弃否定性缓存记录和任何其他动态添加的记录
	/displaydns：显示 DNS 客户解析器缓存的内容，包括从本地主机文件预装载的记录以及由计算机解析的名称查询而最近获得的任何资源记录。DNS 客户服务在查询配置的 DNS 服务器之前使用这些信息快速解析被频繁查询的名称
	/registerdns：初始化计算机上配置的 DNS 名称和 IP 地址的手工动态注册。可以使用该参数对失败的 DNS 名称注册进行疑难解答或解决客户和 DNS 服务器之间的动态更新问题，而不必重新启动客户计算机。TCP/IP 协议高级属性中的 DNS 设置可以确定 DNS 中注册的名称
	/showclassid adapter：显示指定适配器的 DHCP 类别 ID。要查看所有适配器的 DHCP 类别 ID，可以使用星号通配符（*）代替 adapter。该参数仅在具有配置为自动获取 IP 地址的网卡的计算机上可用
	/setclassid adapter [ClassID]：配置特定适配器的 DHCP 类别 ID。要设置所有适配器的 DHCP 类别 ID，可以使用星号（*）通配符代替 adapter。该参数仅在具有配置为自动获取 IP 地址的网卡的计算机上可用。如果未指定 DHCP 类别 ID，则会删除当前类别 ID

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

“命令提示符”命令

命　令	netstat
功　能	显示活动的 TCP 连接、计算机侦听的端口、以太网统计信息、IP 路由表、IPv4 统计信息（对于 IP、ICMP、TCP 和 UDP 协议）以及 IPv6 统计信息（对于 IPv6、ICMPv6、通过 IPv6 的 TCP 以及通过 IPv6 的 UDP 协议）。使用时如果不带参数，netstat 显示活动的 TCP 连接
命令格式	netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]
参数解析	-a：显示所有活动的 TCP 连接以及计算机侦听的 TCP 和 UDP 端口
	-e：显示以太网统计信息，如发送和接收的字节数、数据包数。该参数可以与-s 结合使用
	-n：显示活动的 TCP 连接，不过，只以数字形式表现地址和端口号，却不尝试确定名称
	-o：显示活动的 TCP 连接并包括每个连接的进程 ID（PID）。可以在 Windows 任务管理器中的“进程”选项卡上找到基于 PID 的应用程序。该参数可以与-a、-n 和-p 结合使用
	-p Protocol：显示 Protocol 所指定的协议的连接。在这种情况下，Protocol 可以是 TCP、UDP、TCPv6 或 UDPv6。如果该参数与-s 一起使用按协议显示统计信息，则 Protocol 可以是 TCP、UDP、ICMP、IP、TCPv6、UDPv6、ICMPv6 或 IPv6
	-s：按协议显示统计信息。默认情况下，显示 TCP、UDP、ICMP 和 IP 协议的统计信息。如果安装了 Windows XP 的 IPv6 协议，就会显示有关 IPv6 上的 TCP、IPv6 上的 UDP、ICMPv6 和 IPv6 协议的统计信息。可以使用-p 参数指定协议集
	-r：显示 IP 路由表的内容
	Interval：指定重新显示一次选定的信息需间隔的时间（单位为秒）。按“CTRL+C”组合键停止重新显示统计信息。如果省略该参数，netstat 将只打印一次选定的信息
命　令	ftype
功　能	显示或者修改在文件名扩展关联中使用的文件类型。使用不带参数的 ftype 显示带有已定义的打开命令串的文件类型
命令格式	ftype [FileType[=[OpenCommandString]]]
参数解析	FileType：单击要显示或更改的文件类型
	OpenCommandString：指定打开此类型的文件时要使用的打开命令
命　令	nbtstat
功　能	显示本地计算机和远程计算机基于 TCP/IP 协议的 NetBIOS 统计资料、NetBIOS 名称表和 NetBIOS 名称缓存。nbtstat 可以刷新 netBIOS 名称缓存和注册的 Windows Internet 名称服务（WINS）名称。使用不带参数的 nbtstat 命令将显示帮助
命令格式	NBTSTAT [-a RemoteName] [-A IPAddress] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [Interval]
参数解析	-a RemoteName：显示远程计算机的 NetBIOS 名称表，其中，RemoteName 是远程计算机的 NetBIOS 计算机名称。NetBIOS 名称表是运行在该计算机上的应用程序使用的 NetBIOS 名称列表
	-A IPAddress：显示远程计算机的 NetBIOS 名称表，其名称由远程计算机的 IP 地址指定（以小数点分隔）
	-c：显示 NetBIOS 名称缓存内容、NetBIOS 名称表及其解析的各个地址
	-n：显示本地计算机的 NetBIOS 名称表。Registered 中的状态表明该名称是通过广播或 WINS 服务器注册的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

“命令提示符”命令

命　令	nbtstat
参数解析	-r：显示 NetBIOS 名称解析统计资料。在配置为使用 WINS 的 Windows XP 计算机上，该参数将返回已通过广播和 WINS 解析和注册的名称号码
	-R：清除 NetBIOS 名称缓存的内容并从 Lmhosts 文件中重新加载带有#PRE 标记的项目
	-RR：重新释放并刷新通过 WINS 注册的本地计算机的 NetBIOS 名称
	-s：显示 NetBIOS 客户和服务器会话，并试图将目标 IP 地址转化为名称
	-S：显示 NetBIOS 客户和服务器会话，只通过 IP 地址列出远程计算机
	Interval：指定重新显示选择的统计资料时每次显示之间的秒数。按“CTRL+C”组合键停止重新显示统计信息。如果省略该参数，netstat 将只显示一次当前的配置信息

命　令	tracert
功　能	显示数据包到达目标主机所经过的路径，并显示到达每个节点的时间
命令格式	tracert IP（主机名）[-d] [-h maximum_hops] [-j host-list] [-w timeout]
参数解析	-d：不解析目标主机的地址
	-h maximum_hops：指定搜索到目标地址的最大跳跃数
	-j host-list：按照主机列表中的地址释放源路由
	-w timeout：指定超时时间间隔，程序默认的时间单位是毫秒

命　令	nslookup
功　能	对指定的域名进行 DNS 测试，并反馈相关的信息，供用户查看找出问题所在
命令格式	nslookup 域名

命　令	net
功　能	该命令只能配合后缀参数才能发挥作用，具体对应功能如下
命令格式	net [Accounts \| Computer \| Config \| Continue \| File \| Group \| Help \| Helpmsg \| Localgroup \| Name \| Pause \| Print \| Send \| Session \|Share \| Start \| Statistics \| Stop \| Time \| Use \| User \| View]
参数解析	View：显示域列表、计算机列表或指定计算机的共享资源列表
	User：添加或更改用户账号或显示用户账号信息
	Use：连接或断开计算机与共享资源的连接，或显示计算机的连接信息
	Time：使计算机的时钟与另一台计算机或域的时间同步
	Start：启动服务，或显示已启动服务的列表
	Pause：暂停正在运行的服务
	Continue：重新激活挂起的服务
	Stop：停止 Windows NT/2000/2003 的网络服务
	Share：创建、删除或显示共享资源
	Send：向网络的其他用户、计算机或通信名发送消息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

命　令	net
参数解析	Localgroup：添加、显示或更改本地组
	Group：在 Windows NT/2000/2003 Server 域中添加、显示或更改全局组
	Config：显示当前运行的可配置服务，或显示并更改某项服务的设置
	Computer：从域数据库中添加或删除计算机
	Accounts：更新用户账号数据库、更改密码及所有账号的登录要求

命　令	at
功　能	计划在指定时间和日期，在计算机上运行命令和程序
命令格式	at [\\computername] [[id] [/delete]]
	at [\\computername] time "command"
参数解析	\\computername：要设置任务的计算机名或 IP 地址
	id：任务号
	/ delete：删除任务
	time：设置任务运行时间
	command：设置运行的程序（命令）

命　令	telnet
功　能	允许与使用 Telnet 协议的远程计算机通信
命令格式	telnet[host [port]]
参数解析	host：指定要连接到的 IP 地址
	port：要连接到的端口号

溜客安全网 WwW.176Ku.CoM